Université Grenoble Alpes

M1 Mathématiques Générales

Travail encadré de recherche

Année 2021

Courbes elliptiques : entre algèbre, géométrie et analyse

LOISEL Pierre

Encadré par MACLEAN Catriona

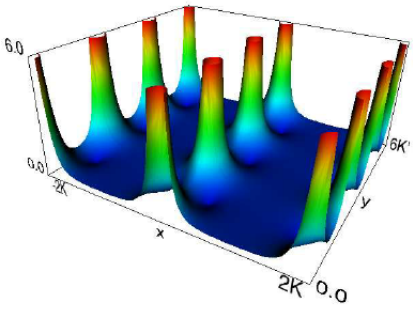

Figure 1 – Module d'une fonction $\wp$ de Weierstrass

Table des matières

0 Introduction **2**

1 Le tore complexe, le point de vue géométrique **3**

1.1 La structure de surface de Riemann du tore complexe 3

1.2 Revêtement universel des tores complexes 5

1.3 Région fondamentale 11

2 Les fonctions $\wp$ de Weierstrass, le point de vue analytique **15**

2.1 Motivation 15

2.2 Définitions et propriétés 16

3 Les cubiques de $\mathbb{P}_2$, le point de vue algébrique **20**

3.1 Le plan complexe projectif $\mathbb{P}_2$ 20

3.2 Courbes projectives complexes 23

3.3 Paramétrisation des cubiques de $\mathbb{P}_2$ par les fonctions de Weierstrass 29

4 Intégration sur une surface de Riemann et théorème de Riemann-Roch **32**

4.1 Différentielle holomorphe et intégration sur les surfaces de Riemann 32

4.2 Le théorème de Riemann-Roch 37

4.3 Démonstration du théorème de Riemann-Roch 40

4.4 Conséquences du théorème de Riemann-Roch 50

A Rappels sur les fonctions holomorphes **53**

B Surfaces de Riemann **54**

0 Introduction

Les courbes elliptiques sont des objets très présent dans le paysage mathématique actuel. Que ce soit par leurs usages en cryptographie ou encore en théorie des nombres, elles sont incontournables. Une courbe elliptique peut être définie de plusieurs manières différentes :

1. Une courbe elliptique une cubique non-singulière du plan projectif complexe $\mathbb{P}_2(\mathbb{C})$.
2. Une courbe elliptique est le quotient de $\mathbb{C}$ par un réseau Λ.
3. Une courbe elliptique est une surface de Riemann homéomorphe à un tore.

Toute ces définitions semblent au premier abord très différentes. Certaines sont de natures algébriques, d'autres géométriques. Pourtant, il n'en est rien ! Toute ces définitions nous donnent en effet le même objet, à savoir une courbe elliptique.

Ce mémoire possède deux objectifs. Le premier est de montrer l'équivalence de ces trois définitions. Cette question occupera les trois premières parties de ce dossier. Dans la première partie, on fera une étude du tore complexe. On y verra notamment que tout tore complexe est bien le quotient de $\mathbb{C}$ par un réseau Λ, et enfin une condition nécessaire et suffisante sur le réseau Λ pour que deux tores complexes soient biholomorphes.

Dans la seconde partie, on introduira les fonctions elliptiques de Weierstrass et on en fera leur étude. Ces fonctions nous serons utiles dans la suite afin de plonger explicitement un tore complexe dans l'espace $\mathbb{P}_2(\mathbb{C})$.

Dans la troisième partie, nous ferons une étude de l'espace projectif $\mathbb{P}_n(\mathbb{C})$ et plus précisément du plan projectif complexe $\mathbb{P}_2(\mathbb{C})$. C'est en effet dans cet espace qu'il est le plus naturel de voir les courbes elliptiques. Par la suite, nous introduirons des notions de géométrie algébrique dont nous aurons besoin, puis nous démontrerons et énoncerons des propriétés et théorèmes sur les courbes projectives complexes. On démontrera, à la fin de cette partie, que tout tore complexe est biholomorphe à une courbe elliptique.

Le second objectif de ce mémoire est de démontrer le théorème de Riemann-Roch dans le cas des courbes de $\mathbb{P}_2(\mathbb{C})$. Nous aurons besoin pour ça d'introduire le concept de différentielle holomorphe et d'intégration sur une surface de Riemann. Nous énoncerons après le théorème et le démontrerons. La principale motivation quant à l'introduction de ce théorème est la suivante : si toute courbe elliptique est le quotient de $\mathbb{C}$ par un réseau, alors toute courbe elliptique possède une structure de groupe induite par celle du tore. Cependant, comment cette loi de groupe se traduit-elle sur une courbe elliptique ? Pouvons-nous réaliser algébriquement cette loi de groupe ? Nous verrons dans une dernière partie comment l'on peut munir toute courbe elliptique d'une loi de groupe. Le théorème de Riemann-Roch nous permettra de montrer que cette loi est bien définie.

1 Le tore complexe, le point de vue géométrique

Nous allons ici proposer une étude des tores complexes. On montrera en première partie que si Λ est un réseau de $\mathbb{C}$, alors $\mathbb{C}/\Lambda$ est un tore munit d'une structure de surface de Riemann. En deuxième partie, on montrera que tout les tores complexes s'expriment comme quotient de $\mathbb{C}$ par un réseau. Enfin, on proposera en dernière partie une classification des tores complexes en tant que point d'une surface (recollée) de $\mathbb{C}$ appelée *région fondamentale*.

La principale motivation de l'étude des tores complexes arrivera en partie 3, où nous montreront qu'il y a une correspondance biholomorphe entre les tores complexes et les cubiques sur $\mathbb{P}_2$.

1.1 La structure de surface de Riemann du tore complexe

Nous allons ici montrer que le quotient de $\mathbb{C}$ par un réseau est une surface de Riemann qui est homéomorphe à un tore. Pour le moment cependant, il n'est pas encore acquis que toute surface de Riemann homéomorphe à un tore est bien le quotient de $\mathbb{C}$ par un réseau. Nous ferons donc, dans cette première partie, la distinction entre le quotient de $\mathbb{C}$ par un réseau et ce que nous appelons un tore complexe (une surface de Riemann homéomorphe à un tore).

Sans plus tarder, introduisons l'objet fondamental de cette première partie, à savoir les réseaux de $\mathbb{C}$.

Définition 1.1.1. *Soient ω_1 et ω_2 deux complexes non-nuls tels que $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. On appelle* réseau de $\mathbb{C}$ engendré par ω_1 et ω_2 *l'ensemble*

$$\Lambda = \{n\omega_1 + m\omega_2, n, m \in \mathbb{Z}\}$$

On notera (ω_1, ω_2) le réseau de $\mathbb{C}$ engendré par ω_1 et ω_2.

On remarque que si l'on considère un réseau Λ, alors il est isomorphe au groupe $\mathbb{Z}^2$ et agit par translation sur $\mathbb{C}$ de manière proprement discontinue et sans point fixe. Comme $\mathbb{C}$ est un groupe abélien, on peut passer au quotient. On obtient ainsi un espace quotient $\mathbb{C}/\Lambda$. Plus exactement, on remarque que $\mathbb{C}/\Lambda$ est homéomorphe à un tore.

Nous allons tout de suite montrer que le tore $\mathbb{C}/\Lambda$ est bien une surface de Riemann [1].

Théorème 1.1.2. *Soit Λ un réseau de $\mathbb{C}$. Le tore $\mathbb{T} = \mathbb{C}/\Lambda$ possède une structure de surface de Riemann.*

Avant de montrer ce théorème, nous aurons besoin d'un lemme préliminaire sur les réseaux et d'un lemme préliminaire sur les tores complexes.

Lemme 1.1.3. *Si ω_1 et ω_2 engendrent le réseau Λ, alors il existe $\delta > 0$ tel que pour tout réels x et y, on a*

$$|x\omega_1 + y\omega_2| \geq \delta\sqrt{x^2 + y^2}$$

1. On renvoie à l'annexe B qui donne les définitions et propriétés fondamentales des Surfaces de Riemann

Démonstration du lemme 1.1.3 : On considère la fonction $f : [0, 2\pi] \longrightarrow \mathbb{R}^+$ définie par

$$f(\theta) = |\cos(\theta)\,\omega_1 + \sin(\theta)\,\omega_2|$$

La fonction f est strictement positive. En effet, si elle s'annule, on aurait $\frac{\omega_1}{\omega_2} \in \mathbb{R}$ ce qui contredirait le fait qu'ils sont des générateurs de Λ. Comme f est continue sur le compact $[0, 2\pi]$, il existe $\delta > 0$ tel que $f(\theta) > \delta$ pour tout $\theta \in [0, 2\pi]$.
Si maintenant x et y sont deux réels, on a

$$|x\omega_1 + y\omega_2| = \sqrt{x^2+y^2} \times \left| \frac{x}{\sqrt{x^2+y^2}}\omega_1 + \frac{y}{\sqrt{x^2+y^2}}\omega_2 \right| \geq \delta\sqrt{x^2+y^2}$$

En effet, on a $\left(\frac{x}{\sqrt{x^2+y^2}}\right)^2 + \left(\frac{y}{\sqrt{x^2+y^2}}\right)^2 = 1$, donc il existe $\theta \in [0, 2\pi]$ tel que $\frac{x}{\sqrt{x^2+y^2}} = \cos(\theta)$ et $\frac{y}{\sqrt{x^2+y^2}} = \sin(\theta)$. □

Lemme 1.1.4. *Soit $\mathbb{T} = \mathbb{C}/\Lambda$ un tore. Alors $\mathbb{T}$ est un espace compact. De plus, la projection canonique π est une application ouverte.*

Démonstration du lemme 1.1.4 : Soit U_a un recouvrement de $\mathbb{T}$ par des ouverts. Notons $\pi : \mathbb{C} \longrightarrow \mathbb{T}$ la projection canonique. Alors $\pi^{-1}(U_a)$ est un recouvrement de $\mathbb{C}$ par des ouverts. Or, si l'on note $\Lambda = (\omega_1, \omega_2)$, alors les ouverts $\pi^{-1}(U_a)$ recouvrent Γ l'enveloppe convexe délimitée par les points $0, \omega_1, \omega_2$ et $\omega_1 + \omega_2$ qui est un compact. Donc Γ est recouvert par un nombre fini d'ouverts de la forme $\pi^{-1}(U_a)$. Or, $\pi(\Gamma) = \mathbb{T}$, d'où le premier résultat.

Soit U un ouvert de $\mathbb{C}$. Alors $\pi^{-1}(\pi(U)) = \bigcup_{\omega\in\Lambda} U + \omega$ est un ouvert de $\mathbb{C}$. Ainsi, $\pi(U)$ est un ouvert de $\mathbb{T}$ par caractérisation de la topologie quotient. □

Démonstration du théorème 1.1.2 : On considère le tore $\mathbb{T} = \mathbb{C}/\Lambda$ munit de la topologie quotient. On notera dans la suite π la projection canonique de $\mathbb{C}$ dans $\mathbb{T}$.

Par le lemme 1.1.3, il existe $\delta > 0$ tel que

$$\forall n, m \in \mathbb{Z} \setminus \{(0,0)\}, \quad |n\omega_1 + m\omega_2| > \delta\sqrt{n^2+m^2}$$

Soit $a \in \mathbb{C}$. On considère la famille d'ouvert de $\mathbb{C}$

$$V_a = \left\{ z \in \mathbb{C} \mid |z-a| < \frac{\delta}{2} \right\}$$

Par le lemme 1.1.4, a restriction de π à l'ouvert V_a induit un homéomorphisme de V_a dans $\pi(V_a)$. Ainsi, la famille $U_a := \pi(V_a)$ est un recouvrement de $\mathbb{T}$. Comme $\mathbb{T}$ est compact, ce recouvrement est fini.

On note $\pi_a = \pi_{|V_a}$ (on a donc π_a qui est un homéomorphisme). On va montrer que $(\pi_a(V_a), \pi_a^{-1})$ est un atlas holomorphe sur $\mathbb{T}$. Ceci impliquera que $\mathbb{T}$ est un espace séparé.

Supposons que $\pi(V_a) \cap \pi(V_b) \neq \emptyset$. Tout d'abord, s'il existe $\omega \in \Lambda$ tel que l'on ait $|\omega + a - b| < \frac{\delta}{2}$, alors cet élément est unique. En effet, si $\omega, \omega' \in \Lambda$ vérifient cette propriété, alors

$$|\omega - \omega'| \leq |\omega + a - b| + |\omega' + a - b| < \delta$$

et on en déduit par le lemme 1.1.3 que $\omega = \omega'$.

Soit maintenant $z \in \pi^{-1}(U_a \cap U_b)$ et $z' = \pi_b^{-1} \circ \pi_a(z)$. On a alors que $\pi(z') = \pi(z)$ et donc que $z' = z + \omega_z$. Mais alors ω_z vérifie $|\omega_z + a - b| < \frac{\delta}{2}$. Ainsi, ω_z ne dépend pas de z et donc l'application $\pi_b^{-1} \circ \pi_a$ est une translation et donc est holomorphe. On a donc que $(\pi(V_a), \pi_a^{-1})$ qu'est bien un atlas holomorphe sur $\mathbb{T}$. □

Ainsi, nous avons montré que le quotient de $\mathbb{C}$ par un réseau est bien une surface de Riemann homéomorphe à un tore. Dans la partie suivante, nous allons montrer la réciproque à savoir que tout tore complexe est bien le quotient de $\mathbb{C}$ par un réseau.

1.2 Revêtement universel des tores complexes

Le but de cette section est de montrer que tout tore complexe est le quotient de $\mathbb{C}$ par un réseau. Pour cela, on utilisera le fait que toute surface de Riemann est le quotient de son revêtement universel par une action de groupe. On verra dans les sous-sections qui viennent que ce revêtement universel est nécessairement biholomorphe à $\mathbb{C}$.

Avant de montrer cela, nous avons besoin de plusieurs définitions et théorèmes de topologie algébrique que nous admettrons. On renverra à [4], page 25 et 63 pour plus de détails concernant les résultats de topologie algébriques que nous admettrons ici.

Définition 1.2.1. *Soit Y une surface de Riemann. On dit que $p : X \longrightarrow X$ est un revêtement de Y si et seulement si pour tout $y \in Y$, il existe un voisinage V de y tel que $p^{-1}(V)$ soit une réunion disjointe d'ouverts U_i et tel que $p_{|U_i} : U_i \longrightarrow V$ soit un biholomorphisme.*

Définition 1.2.2. *Soit Y une surface de Riemann. On dit que le revêtement $p : X \longrightarrow Y$ est un revêtement universel de Y si X est simplement connexe.*

Théorème 1.2.3. *Soit X une surface de Riemann.*

1. *X possède un unique revêtement universel à biholomorphisme près que l'on notera $\tilde{X}$.*
2. *Notons $\pi_1(X)$ le groupe fondamental d'une surface de Riemann X. Alors $\pi_1(X)$ agit de manière proprement discontinue et sans point fixe sur $\tilde{X}$ et $\tilde{X}$ est homéomorphe au quotient de X par $\pi_1(X)$.*
3. *Si X est connexe, alors $\tilde{X}$ est simplement connexe.*

Ainsi, comme le tore $\mathbb{T}$ est connexe par arcs, il possède un unique revêtement universel par le théorème 1.2.3 que l'on notera $\tilde{\mathbb{T}}$. On sait de plus que le groupe fondamental du tore est $\mathbb{Z}^2$. Ainsi, $\mathbb{Z}^2$ agit librement, de manière proprement discontinue et sans point fixe sur $\tilde{\mathbb{T}}$.

On admettra aussi le théorème d'uniformisation de Riemann [2], que nous énonçons ci-dessous.

Théorème 1.2.4. *Soit X une surface de Riemann simplement connexe. Alors X est biholomorphe à l'une des trois surfaces de Riemann ci-dessous :*

1. *Le plan complexe $\mathbb{C}$.*

2. On pourra trouver une preuve de ce théorème dans [5], page 180

2. *La droite projective complexe* $\mathbb{P}_1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$.
3. *Le demi-plan de Poincaré* $H = \{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$.

La suite de cette section aura pour but de montrer que si $\mathbb{T}$ est un tore complexe, alors son revêtement universel est $\mathbb{C}$, et donc que tout tore complexe est de la forme $\mathbb{C}/\Lambda$ avec Λ un réseau. Pour ce faire, nous allons devoir étudier les groupes des biholomorphismes de $\mathbb{C}$, de $\mathbb{P}_1(\mathbb{C})$ et de H et montrer que seul $\mathbb{C}$ possède des biholomorphismes isomorphes à $\mathbb{Z}^2$ qui agissent de manière proprement discontinue et sans points fixes. Notons qu'une telle action de $\mathbb{Z}^2$ est l'action d'un réseau.

Biholomorphismes de $\mathbb{C}$

On va ici déterminer l'ensemble des biholomorphismes de $\mathbb{C}$ ne possédant aucun point fixe. Plus exactement, nous allons montrer le résultat suivant.

Théorème 1.2.5. *Si f est un biholomorphisme de $\mathbb{C}$, alors il existe $a, b \in \mathbb{C}$ avec $a \neq 0$ tels qu $f(z) = az + b$.*

Démonstration On voit directement que les applications de la forme $z \mapsto az + b$ avec $a, b \in \mathbb{C}$ et $a \neq 0$ sont bien des biholomorphismes de $\mathbb{C}$. Soit f un biholomorphisme de $\mathbb{C}$. Alors f possède un développement en série entière donné par

$$f(z) = \sum_{n \geq 0} a_n z^n$$

On considère la fonction $z \mapsto f(\frac{1}{z})$. Cette fonction possède une unique singularité en 0 qui est un pôle d'ordre $k \geq 1$ (en effet, $|f(z)|$ tend vers l'infini en 0). Il existe donc une fonction holomorphe h, bornée au voisinage de 0, telle que

$$f\left(\frac{1}{z}\right) = \frac{h(z)}{z^k}$$

On renvoie à l'appendice A pour plus de détails. Notons $\sum_{n \geq 0} b_n z^n$ le développement en série entière de h au voisinage de 0. On a alors, au voisinage de 0, que

$$\sum_{n \geq 0} b_n z^n = \sum_{n \geq 0} \frac{a_n}{z^{n-k}}$$

Ainsi, on en déduit que $a_n = 0$ pour tout $n \geq k + 1$ et donc que f est un polynôme. Mais comme f est injective, alors on a nécessairement que $k = 1$. Ainsi, $f(z) = a_0 + a_1 z$, qui est bien de la forme que l'on voulait. □

Il est maintenant aisé de trouver les biholomorphismes sans point fixe : ce sont ceux de la forme $z \mapsto z + b$ avec $b \in \mathbb{C}$.

Biholomorphismes de $\mathbb{P}_1(\mathbb{C})$

On va utiliser l'étude des biholomorphismes de $\mathbb{C}$ afin de montrer qu'il n'existe par de biholomorphismes de $\mathbb{P}_1(\mathbb{C})$ sans point fixe. On va tout d'abord montrer que les biholomorphismes de $\mathbb{P}_1(\mathbb{C})$ sont les fonctions de la forme

$$z \mapsto \frac{az+b}{cz+d}$$

où, quitte à diviser par $ad-bc$, on peut prendre $a, b, c, d \in \mathbb{C}$ vérifiant $ad-bc=1$. En effet, une telle fonction est bijective et donc $ad-bc \neq 0$.

Soit f un biholomorphisme de $\mathbb{P}_1(\mathbb{C})$. Si f fixe l'infini, alors f se restreint en un biholomorphisme de $\mathbb{C}$ et on a bien la forme voulu. Sinon, si $x \in \mathbb{C}$ vérifie que $f(x) = \infty$, alors $z \mapsto \frac{1}{f(z)-x}$ est un biholomorphisme qui fixe l'infini, donc est de la forme $az+b$. Ainsi, $f(z) = \frac{axz+bx+1}{az+b}$ et on a bien la forme voulue.

On considère f un tel biholomorphisme. Si $c=0$, alors f fixe l'infini. Si maintenant $c \neq 0$, alors f possède un point fixe dans $\mathbb{C}$ si et seulement si l'équation

$$cz^2 + (d-a)z - b = 0$$

admet des solutions dans $\mathbb{C}$, ce qui est toujours le cas. Donc f possède au moins un point fixe. Ainsi, il n'existe pas de biholomorphisme de $\mathbb{P}_1$ sans point fixe.

Biholomorphismes de H

L'étude des biholomorphismes de H est plus complexe [3] que celle des biholomorphismes de $\mathbb{C}$ et de $\mathbb{P}_1(\mathbb{C})$. Rappelons tout d'abord que le demi-plan de Poincaré H est définie par

$$H = \{z \in \mathbb{C} \mid \mathfrak{Im}(z) > 0\}$$

Nous admettrons que les biholomorphismes de H sont les fonctions

$$z \mapsto \frac{az+b}{cz+d}$$

avec $a, b, c, d \in \mathbb{R}$ vérifiant $ad-bc=1$. On renvoie à [3], page 23, pour une preuve de ce résultat. Nous nous aideront principalement du chapitre 2 de [3] afin de mener à bien cette étude.

Soit f un biholomorphisme de H. Alors z est un point fixe de f si et seulement si z est racine du polynôme

$$P(z) = cz^2 + (d-a)z - b$$

Le cas où ce polynôme possède deux racines non-réelles est directement exclu, car dans ce cas le biholomorphisme aurait un point fixe dans H. Il reste cependant le cas où ce polynôme a une ou deux racines dans $\mathbb{R} \cup \{\infty\}$. On voit donc que l'approche que nous avons eu précédemment ne fonctionne pas et qu'il faut faire autre chose, ce que nous allons faire dans la suite. On a un morphisme de groupe donné par

3. C'est le cas de le dire...

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \left(z \mapsto \frac{az+b}{cz+d} \right)$$

où $a, b, c, d \in \mathbb{R}$ qui vérifient $ad - bc = 1$. Ainsi, le groupe des biholomorphismes de H est isomorphe à un sous-groupe de $\mathrm{SL}_2(\mathbb{R})/\{\pm \mathrm{Id}\}$ que nous noterons $\mathrm{PSL}_2(\mathbb{R})$.

Afin d'étudier ces transformations, nous allons avoir besoin de plusieurs définitions propres aux actions de groupes sur un espace topologique.

Définition 1.2.6. *Soit X un espace topologique et $A \subset X$. On dit que A est localement fini si pour tout $a \in A$, il existe un voisinage U de a tel que $U \cap A$ est fini.*

Définition 1.2.7. *Soit G un groupe topologique agissant sur un espace topologique X. On dit que l'action de G sur X est proprement discontinue si l'orbite de chaque point $x \in X$ est localement finie.*

Définition 1.2.8. *Soit G un sous-groupe de $\mathrm{PSL}_2(\mathbb{R})$. On dira que G est un groupe Fuchsien si G est discret*[4] *et si G agit de manière proprement discontinue sur H.*

Notons que dans toute la suite, nous ferons l'abus qui consiste à identifier un élément $\bar{S} \in \mathrm{PSL}_2(\mathbb{R})$ à son action sur H. Notre étude se ramène donc à la recherche de sous-groupes discrets de $\mathrm{PSL}_2(\mathbb{R})$ agissant sur H de manière proprement discontinue et sans point fixe. On va dans la suite démontrer qu'aucun groupe Fuchsien n'est isomorphe à $\mathbb{Z}^2$. Pour cela, on suivra le cheminement proposé dans [3] au chapitre 2.

Nous allons maintenant introduire du vocabulaire sur les éléments de $\mathrm{PSL}_2(\mathbb{R})$.

Définition 1.2.9. *Soit $S \in \mathrm{PSL}_2(\mathbb{R})$. On dit que S est une transformation (ou matrice) :*
- *elliptique si* $\mathrm{Tr}(S) < 2$.
- *parabolique si* $\mathrm{Tr}(S) = 2$.
- *hyperbolique si* $\mathrm{Tr}(S) > 2$.

Soit $S \in \mathrm{SL}_2(\mathbb{R})$ une transformation hyperbolique. Son polynôme caractéristique est $X^2 - \mathrm{Tr}(S)X + \det(S)$ possède deux racines

$$\frac{-\mathrm{Tr}(S) \pm \sqrt{\mathrm{Tr(S)}^2 - 4}}{2} > 0$$

Ainsi, S possède deux valeurs propres réelles distinctes dont le produit fait 1 et que nous noteront λ et $\frac{1}{\lambda}$. Donc S est conjuguée à la matrice diagonale de diagonale

$$\begin{bmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{bmatrix}$$

et on voit ainsi que S va fixer deux éléments de $\mathbb{R} \cup \{\infty\}$ (rappelons que le nombre de points fixes est stable par conjugaison). On en déduit que toute transformation hyperbolique S est conjuguée à

$$z \mapsto \frac{\lambda z}{\frac{1}{\lambda}} = \lambda^2 z$$

4. En fait, cette hypothèse est superflue. On peut montrer qu'un sous-groupe de $\mathrm{PSL}_2(\mathbb{R})$ est discret si et seulement si son action sur H est proprement discontinue. On trouvera davantage de détails à ce sujet dans [3] p.26.

Donc S est conjuguée à une application de la forme $z \mapsto Cz$ avec $C = \lambda^2$. Une telle transformation possède deux points fixes sur la droite réelle $\mathbb{R}$.

Soit $S \in \mathrm{SL}_2(\mathbb{R})$ une transformation elliptique. Ici, les deux valeurs propres seront complexes et conjuguées, donc S va fixer un élément de H.

Enfin, si $S \in \mathrm{SL}_2(\mathbb{R})$ est une transformation parabolique, le polynôme caractéristique de S une racine double de valeur 1. La matrice S est donc trigonalisable et est conjuguée à un élément de la forme

$$\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$$

avec $b \in \mathbb{R}^*$. Donc une transformation parabolique est conjuguée à

$$z \mapsto \frac{z+b}{1} = z + b$$

qui possède donc un unique point fixe sur $\mathbb{R} \cup \{\infty\}$.

Il faut donc étudier plus en détail le cas des transformations hyperboliques et paraboliques. En effet, leur action sur H est sans point fixe. Nous allons montrer dans la suite qu'un groupe fuchsien ne peut pas être isomorphe à $\mathbb{Z}^2$. Pour ce faire, nous introduisons d'abord un lemme qui nous sera utile dans la suite.

Lemme 1.2.10. *Soient $S, T \in \mathrm{PSL}_2(\mathbb{R})$. Si $ST = TS$, alors S envoie les points fixes de T sur l'ensemble des points fixes de T.*

Démonstration : Soit p un point fixe de T. Alors on a

$$S(p) = ST(p) = TS(p)$$

donc $S(p)$ est bien un point fixe de T. Réciproquement, si p est un point fixe de T, alors $p = S(S^{-1}T(p))$ et $S^{-1}T(p)$ est un point fixe de T (car S et T commutent) et ainsi tout point fixe de T est de la forme $S(p)$ □

On va maintenant pouvoir montrer une condition nécessaire et suffisante pour que deux éléments de $\mathrm{PSL}_2(\mathbb{R})$ commutent.

Propriété 1.2.11. *Soient $S, T \in \mathrm{PSL}_2(\mathbb{R})$ distincts de $\pm I$. Alors on a $ST = TS$ si et seulement si S et T ont les mêmes ensembles de points fixes.*

Démonstration : Supposons que $S, T \in \mathrm{PSL}_2(\mathbb{R})$ commutent et sont distincts de l'identité. Si T est parabolique, S aura un unique point fixe. En effet, supposons que S possède deux points fixes notés z_1 et z_2. Alors l'un des deux, par exemple z_1 est un des points fixes de T par le lemme 1.2.9. Mais on sait que T envoie les points fixes de S sur les points fixes de S. Comme T est une bijection, on a nécessairement $T(z_2) = x_2$. Or, T est différente de l'identité et est une transformation parabolique. Ainsi, S ne peut posséder qu'un point fixe et est donc parabolique. Le lemme 1.2.9 donne ainsi que S et T ont le même point fixe.

Si T est hyperbolique, supposons par l'absurde que S n'a pas le même ensemble de point fixe. Supposons dans un premier temps que S^2 est l'identité. Alors $X^2 - 1$ est annulateur de S et donc $S = \pm I$ ce qui est absurde (T ne peut pas être conjugué à $-I$ comme $\det(T) = 1$).

Si S^2 est différente de l'identité, alors nécessairement S échange les deux points fixes de T. Or, cela voudrait dire que S^2 aurait trois points fixes, ce qui est impossible. Donc S et T ont les mêmes ensembles de points fixes.

Si T est elliptique, alors T a un unique point fixe dans H, qui sera par conséquent aussi un point fixe pour S, donc T et S fixent les mêmes éléments par le lemme 1.2.9. Ainsi, si deux éléments commutent, ils auront bien les mêmes ensembles de points fixes.

On va maintenant montrer la réciproque de la proposition. Si S et T sont deux éléments possédant les mêmes ensembles de points fixes.

Supposons que T soit parabolique et soit z_0 son point fixe. Alors il existe une transformation $M \in \mathrm{PSL}_2(\mathbb{R})$ telle que $MTM^{-1} : z \mapsto z+a$ pour $a \neq 0$ (rappelons que S et T sont distincts de l'identité). On a donc, comme MTM^{-1} fixe l'infini, que $M(\infty) = z_0$. Ainsi, on a que $M^{-1}SM(\infty) = \infty$, donc $M^{-1}SM$ est une transformation de la forme $z \mapsto z + b$ avec $b \neq 0$. Or, on voit directement que les transformation $z \mapsto z + a$ et $z \mapsto z + b$ commutent. On en déduit ainsi que T et S commutent.

Supposons maintenant que T soit hyperbolique et notons ses points fixes z_1 et z_2. Il existe donc $M \in \mathrm{PSL}_2(\mathbb{R})$ telle que $MTM^{-1} : z \mapsto \lambda z$ avec $\lambda \neq 1$, donc MTM^{-1} fixe 0 et l'infini. De ces relations, on en déduit que M envoie z_1 et z_2 sur l'infini et sur $x \in \mathbb{R}$. Ainsi, $M^{-1}SM$ fixe l'infini et 0, donc $M^{-1}SM$ est de la forme $z \mapsto \mu z$, et donc T et S commutent. On admettra que cette proposition est aussi vrai dans le cas où T est elliptique (nous n'en avons en réalité pas besoin, comme nous le verrons dans la suite). □

On a quasiment tout les éléments pour montrer qu'un groupe Fuchsien ne peut être isomorphe à $\mathbb{Z}^2$. Avant cela, nous auront besoin d'un résultat sur les sous-groupes discrets de $\mathbb{R}$.

Lemme 1.2.12. *Si G est un sous-groupe discret non-trivial de $\mathbb{R}$, alors G est monogène.*

Démonstration : Comme G est un sous-groupe discret, $G \cap \mathbb{R}_+^*$ possède un plus petit élément que l'on note x. On a clairement que $x\mathbb{Z} \subset G$. Supposons qu'il existe $y \in G$ tel que $y \notin x\mathbb{Z}$. Quitte à considérer $-y$, on peut supposer $y > 0$. Alors, comme $\mathbb{R}$ est archimédien, il existe $n \in \mathbb{N}$ tel que

$$nx < y < (n+1)x$$

mais alors $y - nx \in G$ et $0 < y - nx < x$, ce qui contredit la minimalité de x. Donc G est monogène. □

On va maintenant pouvoir montrer, avec tout ce que nous venons de montrer, que tout groupe fuchsien dont tout les éléments ont les mêmes points fixes est cyclique. Dans notre étude, nous pouvons nous limiter au cas où le groupe ne contient que des éléments hyperboliques ou paraboliques, le cas des éléments elliptiques ayant été traité au début de cette partie.

Théorème 1.2.13. *Soit G un groupe fuchsien dont tout les éléments non-triviaux ont les mêmes points fixes. Alors G est monogène.*

On donne tout de suite les deux corollaires importants de ce théorème avant de le démontrer.

Corollaire 1.2.14. *Tout groupe fuchsien abélien est monogène.*

Démonstration : Soit G un groupe fuchsien abélien. Par la proposition 2.3.8, tout les éléments de G ont les mêmes points fixes, donc par le théorème 2.3.10, on en déduit directement que G est monogène. □

Corollaire 1.2.15. *Il n'existe pas de groupe fuchsien isomorphe à $\mathbb{Z}^2$. Ainsi, il n'existe pas de sous-groupe discret de H agissant sans point fixe et de manière proprement discontinue.*

Démonstration du théorème : Montrons en premier lieu que $\mathrm{PSL}_2(\mathbb{R})$ est 2-transitif. Rappelons qu'un groupe G agit de manière 2-transitive sur un ensemble X si pour tout $x \neq y \in X$, pour tout $a \neq b \in X$, il existe $g \in G$ tel que $g \cdot x = a$ et $g \cdot y = b$. Pour montrer que $\mathrm{PSL}_2(\mathbb{R})$ agit de manière 2-transitive sur H, il suffit de montrer que l'on peut envoyer toute paire d'élément sur la paire $(0, \infty)$. Or, il est clair que si $x, y \in H$, l'application

$$z \mapsto \frac{z - x}{z - y}$$

envoie la paire (x, y) sur $(0, \infty)$.

Soit G un groupe fuchsien dont tout les éléments non-triviaux ont les mêmes points fixes. Dans ce cas, grâce à la classification des éléments de $\mathrm{PSL}_2(\mathbb{R})$, tout les éléments de G sont du même type. On ne montrera le théorème que dans le cas où G possède des éléments hyperboliques ou paraboliques (pour notre étude, nous n'avons pas à traiter le cas elliptique).

Supposons que tout les éléments de G sont hyperboliques et notons z_1, z_2 leurs points fixes communs. Quitte à conjuguer le groupe par un élément, on peut supposer que tout les éléments de G fixent l'infini et 0. Ainsi, G est un sous-groupe discret du groupe $K = \{z \mapsto \lambda z \mid \lambda > 0\}$ qui est isomorphe à un sous-groupe discret de $\mathbb{R}^*$, lui-même isomorphe à un sous-groupe discret de $\mathbb{R}$ par l'isomorphisme de groupe topologique $x \mapsto \ln(x)$. Ainsi, par le lemme 1.2.9, on en déduit que G est monogène.

Supposons maintenant que tout les éléments de G sont paraboliques. Quitte à conjuguer le groupe par un élément, on peut supposer que tout les éléments de G fixent l'infini. Alors G est un sous-groupe discret de $K = \{z \mapsto z + b \mid b \in \mathbb{R}\}$ et on conclue de la même manière que dans le cas hyperbolique. □

Ainsi, si $\mathbb{T}$ est un tore complexe, alors $\mathbb{T}$ est nécessairement le quotient de $\mathbb{C}$ par un groupe isomorphe à $\mathbb{Z}^2$, c'est à dire un réseau.

1.3 Région fondamentale

L'objectif de cette section est de chercher à savoir sous quelles conditions deux tores complexes sont biholomorphes. Nous avons vu précédemment qu'à un réseau, on pouvait associer un tore complexe. Nous allons voir maintenant à quelle condition deux réseaux donnent le même tore complexe [5], puis nous allons voir qu'il est possible de "classifier" tout les tores complexes en les voyant comme une partie de $\mathbb{C}$ que l'on aura recollé.

5. On entend ici que les deux réseaux vont donner deux tores qui sont biholomorphes.

Nous aurons besoin avant cela d'un théorème que nous allons admettre sur les revêtements universels de deux surfaces de Riemann biholomorphe.

Théorème 1.3.1. *Soient X et X' deux surfaces de Riemann biholomorphes et notons leurs revêtements universels $\tilde{X}$ et $\tilde{X}'$. Alors $\tilde{X}$ et $\tilde{X}'$ sont biholomorphes.*

On commence par une proposition qui nous dit quand est-ce que deux réseaux sont associés au même tore.

Propriété 1.3.2. *Soit Λ et Λ' deux réseaux tels que $\mathbb{C}/\Lambda$ est biholomorphe à $\mathbb{C}/\Lambda'$. Alors il existe $a \in \mathbb{C}$ tel que $\Lambda' = a\Lambda$.*

Démonstration : Si $\mathbb{C}/\Lambda$ est biholomorphe à $\mathbb{C}/\Lambda'$, par le théorème 1.3.1, il existe un biholomorphisme f de $\mathbb{C}$ qui envoie Λ sur Λ' [6] et qui vérifie $f(0) = 0$. Mais par le théorème 3.1.3, il existe $a, b \in \mathbb{C}$ tels que $f(z) = az + b$ avec $a \neq 0$. On a ainsi $\Lambda' = a\Lambda$. □

Ainsi, on dira que deux réseaux sont équivalents si ces derniers engendrent le même tore complexe. Avant de continuer notre étude, nous allons avoir besoin d'un lemme sur les réseaux qui nous permettra de parler de la région fondamentale. Tout d'abord, notons que par multiplication par un complexe de la forme $ae^{i\theta}$, on peut toujours se ramener au cas où le réseau Λ est de la forme $(1, \omega)$ où 1 est le plus petit vecteur en module du réseau.

Lemme 1.3.3. *Soit Λ un réseau de $\mathbb{C}$ et τ le plus petit vecteur en module de Λ qui ne soit pas colinéaire à 1 et qui est de module ≥ 1. Alors $(1, \tau) = \Lambda$.*

Démonstration : Soit $v \in \Lambda$. On considère ici 1 et τ comme deux vecteurs de $\mathbb{R}^2$. Ainsi, $(1, \tau)$ est une base de $\mathbb{R}^2$ et il existe donc $a, b \in \mathbb{R}$ tels que $v = a + b\tau$. On note p_a (resp p_b) la partie entière de a (resp de b) et on note aussi r_a (resp r_b) la partie fractionnaire de a (resp de b).

Supposons dans un premier temps qu'il n'y a aucun vecteur de Λ dans le parallélogramme engendré par 1 et par τ. Alors $p_a + p_b\tau$ est un vecteur du réseau et donc il en est de même pour $v - (p_a + p_b\tau = r_a + r_b\tau$. Or, $r_1 < 1$ et $r_b < 1$, donc $r_a + r_b\tau$ se trouve dans le parallélogramme formé par 1 et τ. La seule possibilité est que $r_a = r_b = 0$.

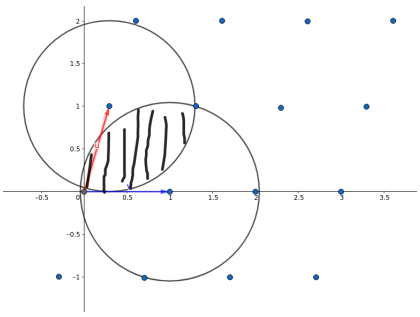

FIGURE 2 – Dessin de la situation décrite dans la démonstration du lemme 1.3.3.

Montrons qu'il n'y a qu'un seul point dans le parallélogramme formé par $(1, \tau)$. On considère $\mathcal{D}_1$ le disque de centre $(1, 0)$ et de rayon $|\tau|$. On considère de même $\mathcal{D}_\tau$ le disque de centre τ de rayon

6. Un tel f existe : il faut considérer un biholomorphisme $\tilde{f}$ de $\mathbb{C}/\Lambda$ sur $\mathbb{C}/\Lambda'$ puis de le relever en un biholomorphisme f de revêtements universels puis le translater afin que $f(0) = 0$.

1. Le disque $\mathcal{D}_1$ ne peut contenir, en dehors de sa frontière, que des multiples de 1. En effet, si ce n'était pas le cas, on trouverait un vecteur du réseau non-colinéaire à 1 de norme strictement plus petite à celle de τ. De même, il n'y a aucun vecteur dans l'intérieur de $\mathcal{D}_\tau$, sinon il existerait des vecteurs du réseau de norme strictement plus petite que 1. De plus, si v est un vecteur de l'intérieur du parallélogramme, alors v est dans l'intérieur d'un des deux disques (c.f figure 2).

Ainsi, il n'y a aucun vecteurs dans l'intérieur du parallélogramme $(1, \tau)$, et quatre vecteurs du réseau formant les sommets du parallélogramme : 0, 1, τ et $1 + \tau$. □

À partir de maintenant, τ désignera le plus petit vecteur en norme qui ne soit pas colinéaire à 1. Quitte à translater de nouveau le vecteur τ à droite ou à gauche par $1 \times n$, on peut supposer que la partie réelle de τ est comprise entre $-\frac{1}{2}$ et $\frac{1}{2}$. Ainsi, tout réseau de $\mathbb{C}$ dont le plus petit élément est 1 est représenté par un vecteur se trouvant dans une région Γ définie par

$$\Gamma = \left\{ \tau \in \mathbb{C} \mid |\tau| \geq 1,\ \mathrm{Im}(\tau) > 0 \text{ et } \mathrm{Re}(\tau) \in \left]-\frac{1}{2}, \frac{1}{2}\right] \right\}$$

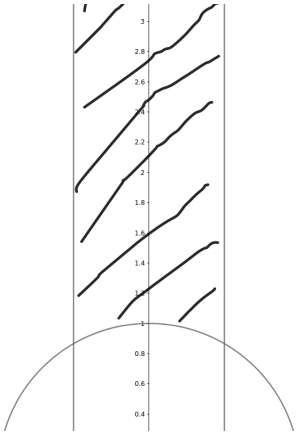

FIGURE 3 – *La région Γ, hachurée en noir*

On va montrer que si Λ est engendré par 1 et par un vecteur $\tau \in \Gamma$, alors τ est de norme minimal (en dehors des éléments engendrés par 1).

Propriété 1.3.4. *Soit $\tau \in \Gamma$ et soit $\Lambda = (1, \tau)$ un réseau. Alors τ est le plus petit élément de Λ qui ne soit pas dans (1).*

Démonstration : Raisonnons par l'absurde et supposons qu'il existe un élément $v \in (1, \tau)$ vérifiant $|\tau| > |v|$. Comme $(1, \tau)$ engendre Λ et que $|\tau| \geq 1$, on a pour tout $n \in \mathbb{Z} \setminus \{0\}$ et pour tout $m \in \mathbb{Z}$

$$|n\tau + m| \geq |\tau|$$

Mais alors on a, comme $v \in \Lambda$, que $|v| \geq |\tau|$, ce qui est absurde. □

Une première condition nécessaire pour que $(1, \tau_1) \sim (1, \tau_2)$ qui découle directement de proposition est que $|\tau_1| = |\tau_2|$. Il faut cependant traiter à part le cas où le complexe τ est de module 1.

Propriété 1.3.5. *Soient $\tau_1, \tau_2 \in \Gamma$ tels que $(1, \tau_1) \sim (1, \tau_2)$ et que τ_1 et τ_2 soient les vecteurs minimaux de leurs réseau respectif non-colinéaires à 1. Supposons de plus que $|\tau_1| = 1$. Alors $\tau_1 = \tau_2$ ou $\tau_2 = -\overline{\tau_1}$.*

Démonstration : Soit $\Lambda_1 = (1, \tau_1)$ et $\Lambda_2 = (1, \tau_2)$. Supposons tout d'abord que Λ_1 est le réseau hexagonal. Alors il y a un unique vecteur de Λ_1 et Λ_2 de norme 1 dans Γ (il est de partie réelle $\frac{1}{2}$ et de norme 1) et donc $\tau_1 = \tau_2$.

Supposons qu'aucun de ces réseaux ne soit le réseau hexagonal. Alors le cardinal de l'ensemble $\Lambda_1 \cap \mathbb{S}$ (où $\mathbb{S}$ est le cercle unité de $\mathbb{C}$) est 4. En effet, par l'absurde, supposons que son cardinal soit strictement plus grand que 4. Alors comme Λ_1 n'est pas le réseau hexagonal et que $\tau_1 \in \Gamma$, on a $\arg(\tau_1) \in \left]\frac{\pi}{3}; \frac{2\pi}{3}\right[$. Ainsi, $\mathrm{Re}(\tau_1) < \frac{1}{2}$. Un élément de norme 1 vérifie alors qu'il existe $m, n \in \{0, \pm 1\}$ tels que $|m\tau_1 + n| = 1$. Si $m = 0$, on trouve $n = 1$ ou $n = -1$. Sinon, si $m = 1$, alors $n = \pm 1$ et $|\mathrm{Re}(\tau_1 \pm 1)| = |\mathrm{Re}(\tau_1)|$. Mais $|\mathrm{Re}(\tau_1 \pm 1)| = |\mathrm{Re}(\tau_1) \pm 1| = |\mathrm{Re}(\tau_1)|$ et donc $\mathrm{Re}(\tau_1) = \pm\frac{1}{2}$ ce qui donne que le réseau est hexagonal, ce qui est absurde.

Ainsi, il n'y a que 4 éléments de norme 1 : ± 1 et $\pm\tau_1$. Supposons maintenant que $\Lambda_1 = \Lambda_2$. Alors il existe $a \in \mathbb{C}$ de norme 1 tel que $a(1, \tau_1) = (1, \tau_2)$. Si $a \times 1$ est envoyé sur 1, alors $a = 1$ et $\tau_1 = \tau_2$. Supposons que $a \times 1 = \tau_2$. Alors $\tau_1 \times \tau_2 = \pm$ et donc $\tau_1 = \pm\bar{\tau_2}$. □

Ainsi, les ensembles

$$\Gamma \cap \{\mathrm{Re}(\tau) \leq 0 \text{ et } |\tau| = 1\} \text{ et } \Gamma \cap \{\mathrm{Re}(\tau) \geq 0 \text{ et } |\tau| = 1\}$$

qui sont des arcs de cercle, nous donnent les mêmes réseaux. La propriété 1.3.5 n'est cependant plus vraie lorsque l'on considère des réseaux vérifiant $\tau_1 > 1$.

Propriété 1.3.6. *Soient $\tau_1, \tau_2 \in \Gamma$ tels que $(1, \tau_1) \sim (1, \tau_2)$. Supposons de plus que $|\tau_1| > 1$. Alors $\tau_1 = \tau_2$.*

Démonstration : Supposons que $(1, \tau_1) \sim (1, \tau_2)$. Soit $a \in \mathbb{C}$ tel que $(1, \tau_2) = a(1, \tau_1)$. Si $|a| = 1$, alors 1 est envoyé sur un vecteur de longueur 1 de $(1, \tau_2)$ et donc $a = \pm 1$ et ainsi $\tau_1 = \tau_2$.

Supposons que $|a| > 1$. Alors, comme 1 est de norme minimal dans $(1, \tau_1)$, on a pour tout $\omega \in (1, \tau_1)$ que $|a\omega| > 1$ et donc $1 \in (1, \tau_2)$ n'est l'image d'aucun vecteur de $(1, \tau_1)$. Ainsi, on a nécessairement que $\tau_1 = \tau_2$. □

On appellera ainsi région fondamentale la région Γ où on a recollé les demi-droite de partie réelle $\pm\frac{1}{2}$ et où on a aussi recollé les deux arcs de cercles de Γ de module 1 de manière symétrique. Le recollement des arcs de cercle vient de la propriété 1.3.4. Le recollement des demis-droites vient du fait que si $\mathrm{Re}(\tau) = \frac{1}{2}$, alors $\tau - 1 \in (1, \tau)$ est de même norme que τ.

2 Les fonctions $\wp$ de Weierstrass, le point de vue analytique

Le but de cette section est de pouvoir immerger un tore complexe dans $\mathbb{P}_2(\mathbb{C})$ afin de montrer que tout tore complexe est une cubique de $\mathbb{P}_2(\mathbb{C})$. La démonstration repose sur les fonctions $\wp$ de Weierstrass, dont nous allons démontrer plusieurs propriétés dans cette section avant d'y revenir plus loin dans la partie 3.3.

2.1 Motivation

Soit $\mathbb{C}/\Lambda$ un tore complexe. Il est facile de voir qu'une fonction $f : \mathbb{T} \longrightarrow \mathbb{C}$ est holomorphe si et seulement si $f \circ \pi$ est holomorphe aussi. Ainsi, les fonctions holomorphes du tore correspondent aux fonctions doublements périodiques de $\mathbb{C}$. Il est donc naturel d'essayer de les chercher.

Tout d'abord, si f est doublement périodique et est holomorphe, le théorème de Liouville implique qu'une telle fonction est constante. Pour en trouver, il faut donc être moins restrictif et se permettre de considérer des fonctions méromorphes. Ces dernières ne seront pas entièrement définies sur $\mathbb{C}$ et à valeur dans $\mathbb{C}$, mais nous contourneront cette difficulté dans la section 3 en introduit le plan projectif complexe $\mathbb{P}_2$.

Essayons de construire une fonction f doublement périodique qui cette fois serait méromorphe. Soit f une fonction méromorphe possédant un unique pôle (par exemple en 0), puis posons la fonction

$$g(z) = \sum_{(n,m)\in\mathbb{Z}^2} f(z - n\omega_1 - m\omega_2)$$

pour peu que f possède de bonnes propriétés de sommabilité, la fonction g sera méromorphe sur $\mathbb{C}$, ne sera pas constante et sera du type que l'on cherche. Reste à trouver une telle fonction f. Considérons la fonction $f(z) = \frac{1}{z^k}$ avec k un entier. Si $k > 2$, notre fonction g sera bien définie. Par contre, elle ne sera pas bien définie pour $k = 2$. Mais si l'on introduit un terme correctif, alors la fonction

$$g(z) = \frac{1}{z^2} + \sum_{(n,m)\in\mathbb{Z}^2} \frac{1}{(z - n\omega_1 - m\omega_2)^2} - \frac{1}{(n\omega_1 + m\omega_2)^2}$$

est bien définie, méromorphe sur $\mathbb{C}$, invariante par l'action d'un réseau et elle possède un pôle double aux points du réseau. Cette section servira à montrer cela.

Qu'en est-il du cas $k = 1$? De manière plus générale, peut-on trouver une fonction méromorphe invariante sous l'action d'un réseau et qui possède un unique pôle simple dans un parallélogramme ? La réponse est négative. En effet, si une telle fonction méromorphe f existait, alors en considérant un parallélogramme autour d'un de ses pôles, de sorte à ce qu'il y en ai qu'un seul, on aurait d'une part, par le théorème des résidus, que son intégrale sur ce parallélogramme est non-nulle. Mais comme f est doublement périodique, cette intégrale sera en fait nulle, ce qui est contradictoire.

Ainsi, on va définir les fonctions $\wp$ de Weierstrass comme étant des fonctions méromorphes sur $\mathbb{C}$ doublement périodiques qui possèdent un unique pôle double en 0.

2.2 Définitions et propriétés

On suivra ici le cheminement proposé dans [1] p.115.

Définition 2.2.1. *Soit Λ un réseau de $\mathbb{C}$. On définit une fonction méromorphe sur $\mathbb{C}$ en posant*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

La fonction φ est appelée fonction de Weierstrass associée au réseau Λ *ou encore* fonction elliptique de Weierstrass associée au réseau Λ. *De plus, elle vérifie*

$$\wp'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z-\omega)^3}$$

Démonstration : La fonction $z \longrightarrow \frac{1}{z^2}$ est méromorphe sur $\mathbb{C}$. Il suffit donc de montrer que

$$\sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

définit bien une fonction méromorphe sur $\mathbb{C}$. Afin de montrer cela, on va appliquer le critère de Weierstrass en montrant que pour tout $R > 0$, il existe un ensemble fini Λ_R tel que la série

$$\sum_{\omega \in \Lambda \setminus \Lambda_R} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

converge uniformément sur le disque fermé $\{|z| \leq R\}$. Posons

$$\Lambda_R = \{\omega \in \Lambda \mid |\omega| \leq 2R\}$$

On a alors l'inclusion que

$$\Lambda_R \subset \left\{ n\omega_1 + m\omega_2, n, m \in \mathbb{Z} \text{ et } n^2 + m^2 \leq \frac{4R^2}{\delta^2} \right\}$$

En effet, si $\omega = n\omega_1 + m\omega_2 \in \Lambda_R$, on a par le lemme 1.1.3 que

$$2R \geq |\omega| \geq \delta\sqrt{n^2+m^2}$$

Et donc, en élevant au carré, on obtient bien que $n^2 + m^2 \leq \frac{4R^2}{\delta^2}$. Ainsi, Λ_R est bien fini.

On va donc majorer le terme général de $\displaystyle\sum_{\omega \in \Lambda \setminus \Lambda_R} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$. Remarquons que l'on a $|z| \leq \frac{|\omega|}{2}$. Ainsi, on peut majorer le terme général de la série de la façon suivante :

$$\begin{aligned} \left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| &= \frac{|z(2\omega - z)|}{|\omega^2(z-\omega)^2|} \\ &\leq \frac{10R}{|\omega|^3} \\ &\leq \frac{10R}{\delta^3} \times \frac{1}{(n^2+m^2)^{\frac{3}{2}}} \end{aligned}$$

Il suffit donc de regarder la convergence ou la divergence de la série de terme générale $\frac{1}{(n^2+m^2)^{\frac{3}{2}}}$. Mais on a

$$\begin{aligned}
\sum_{(m,n)\neq 0} \frac{1}{(n^2+m^2)^{\frac{3}{2}}} &= \sum_{k\geq 1} \sum_{\max(|n|,|m|)=k} \frac{1}{(n^2+m^2)^{\frac{3}{2}}} \\
&= 4\sum_{k\geq 1} \sum_{\max(|n|,|m|)=k \text{ et } n,m\geq 1} \frac{1}{(n^2+m^2)^{\frac{3}{2}}} \\
&\leq 4\sum_{k\geq 1} \left(\frac{1}{k^3} \sum_{\max(|n|,|m|)=k \text{ et } n,m\geq 1} 1 \right) \\
&= 8\sum_{k\geq 1} \frac{1}{k^2}
\end{aligned}$$

On obtient ainsi par le critère de Riemann le résultat. □

Propriété 2.2.2. *Soit Λ un réseau de $\mathbb{C}$ et $\wp$ la fonction de Weierstrass associée à ce réseau.*

1. *La fonction $\wp$ est paire.*
2. *Pour tout $\xi \in \Lambda$ et $z \in \mathbb{C}$, $\wp(z+\xi) = \wp(z)$.*

Démonstration :

1. On a

$$\begin{aligned}
\wp(-z) &= \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \\
&= \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \\
&= \wp(z)
\end{aligned}$$

2. On ne peut pas directement réarranger les termes de la somme dans $\wp(z+\xi)$ car l'on ne sait pas si cette somme est absolument convergente. Pour contourner ce problème, on va travailler sur $\wp'$ qui elle est absolument convergente.

   On a directement que pour tout $\xi \in \Lambda$, $\wp'(z+\xi) = \wp'(z)$ et ce pour tout $z \in \mathbb{C}$. On a alors que $\wp(z+\xi) = \wp(z) + c(\xi)$ où c est une fonction ne dépendant que de ξ. Mais ceci est vrai pour tout $z \in \mathbb{C}$. En évaluant en $\frac{-\xi}{2}$ et en utilisant la périodicité de $\wp$, on obtient le résultat attendu. □

La propriété qui vient est fondamentale. C'est elle qui nous permettra de paramétriser les courbes elliptiques par une certaine fonction de Weierstrass associée à un réseau.

Propriété 2.2.3. *La fonction $\wp$ associée au réseau Λ vérifie l'équation différentielle*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

où les quantités g_2 et g_3, qui dépendent du réseau Λ, sont données par

$$g_2 = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}$$
$$g_3 = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$$

Démonstration : La fonction $\wp(z) - \frac{1}{z^2}$ est définie en dehors de 0 et tend vers 0 en 0. De plus, elle est paire (par parité de $\wp$). Donc $\wp$ possède donc un développement limité en 0 et on a

$$\wp(z) = \frac{1}{z^2} + \lambda z^2 + \mu z^4 + z^6 h(z)$$

avec h une fonction holomorphe définie au voisinage de 0 et λ, $\mu \in \mathbb{C}$. On a donc aussi

$$\wp(z)' = \frac{-2}{z^3} + 2\lambda z + 4\mu z^3 + 6z^5 h(z) + z^6 h'(z)$$

On considère alors la fonction $k(z) = \wp'(z)^2 - 4\wp(z)^3 + g_2\wp(z) + g_3$ avec $g_2 = 20\lambda$ et $g_3 = 28\mu$.
Au voisinage de 0, on a

$$\wp(z)^3 = \frac{1}{z^6} + \frac{3\lambda}{z^2} + 3\mu + o(z)$$
$$\wp'(z)^2 = \frac{4}{z^6} - \frac{8\lambda}{z^2} - 16\mu + o(z)$$

Ainsi, au voisinage de 0, on a que $k(z) = o(z)$, d'où $k(0) = 0$. Mais, comme $\wp$ est doublement périodique, on a alors que k est une fonction holomorphe qu'est doublement périodique. Donc $k = 0$ et on a bien l'égalité $\wp'(z) = 4\wp(z)^2 - g_2\wp(z) - g_3$.
Pour trouver les expressions de g_2 et g_3, on remarque que λ est la valeur de la seconde dérivée de $\sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^2}$ en 0, et que g_3 est la valeur de la dérivée quatrième en 0. □

Propriété 2.2.4. *La fonction $\wp : \mathbb{C} \setminus \Lambda \longrightarrow \mathbb{C}$ est surjective. De plus, on a $\wp(z) = \wp(z')$ si et seulement si $z \in \Lambda \pm z'$.*

Démonstration : Soit $c \in \mathbb{C}$ et ω_1, ω_2 les deux générateurs du réseau Λ. On considère la fonction f définie par $f(z) = \wp(z) - c$. Alors, parle théorème de l'indice, $\frac{f'}{f}$ a des pôles simples aux points de Λ. Soit γ le lacet délimitant le parallélogramme $\mathcal{P}(a) = \{a + s\omega_1 + t\omega_2 \mid s, t \in [0,1]\}$, avec a choisi de sorte à ce que le bord du parallélogramme ne rencontre aucun point de Λ. Ainsi, on voit qu'il existe un unique $\xi \in \mathcal{P}(a) \cap \Lambda$. On a donc d'une part, par le théorème de l'indice, que

$$\frac{1}{2i\pi} \int_\gamma \frac{f'(z)}{f(z)} dz = Z - P$$

et, d'autre part, comme f et f' sont aussi doublement périodiques, on a que

$$\int_\gamma \frac{f'(z)}{f(z)} dz = 0$$

et ainsi $Z = P$. Mais on sait que $\wp$ n'a que des pôles d'ordre 2. Ainsi, comme on a un unique $\xi \in \mathcal{P}(a) \cap \Lambda$, on a $P = 2$, d'où $Z = 2$ et ainsi $\wp$ est surjective.

Notons w_0 un zéro de f. Par double périodicité de $\wp$, on sait que l'on a $\wp(w_0) = \wp(z) = c$ pour tout $\forall z \in \Lambda \pm w_0$. On a ainsi la condition suffisante de l'énoncé. Montrons que cette condition est nécessaire.

Par l'étude ci-dessus, il existe un élément $w_1 \in \mathcal{P}(a)$ tel que $f(w_1) = 0$. Si $w_0 \neq w_1$, alors on a nécessairement que $w_1 \in \Lambda \pm w_0$. Si $w_0 = w_1$, il faut montrer que w_0 est un zéro double de f. Mais $\wp'$ est une fonction doublement périodique et impaire. Donc $\wp'(w_0) = -\wp(-w_0) = -\wp(w_0)$, e donc $\wp'(w_0) = 0$, d'où $f'(w_0) = 0$. □

On aimerait pouvoir complètement paramétriser les courbes elliptiques à l'aide des fonctions $\wp$. Seulement, pour cela, nous avons besoin de compacité. On a déjà rencontré ce problème lorsque l'on cherchait des fonctions doublements périodiques du tore dans $\mathbb{C}$. En effet, si l'on veut que $\wp$ puisse paramétriser un tore complexe, on va avoir un problème avec les points envoyés à l'infini. Il nous faut donc rendre compact $\mathbb{C}$, ce qui nous amène à la troisième section de ce mémoire.

3 Les cubiques de $\mathbb{P}_2$, le point de vue algébrique

Dans cette partie, nous commencerons par définir le plan projectif complexe $\mathbb{P}_2$, puis nous introduirons des notions élémentaires de géométrie algébrique afin de pouvoir définir ce que sont les courbes projectives complexes. On verra enfin que l'on peut paramétrer de manière biholomorphes une cubique sur un tore complexe à l'aide des fonctions de Weierstrass.

3.1 Le plan complexe projectif $\mathbb{P}_2$

Dans toute la suite, $\mathbb{C}^{n+1}$ sera muni de sa topologie usuelle.

Définition 3.1.1. *Soit $n \geq 1$ un entier. On appelle espace projectif complexe de dimension n, noté $\mathbb{P}_n$, l'ensemble des sous-espaces vectoriels de dimension 1 de $\mathbb{C}^{n+1}$. Si $n = 1$, on l'appellera la droite projective complexe. Si $n = 2$, on l'appellera le plan projectif complexe.*

Définition 3.1.2. *Soit $n \geq 1$. $u = (x_0, \ldots, x_n) \in \mathbb{C}^{n+1} \setminus \{0\}$ représente un unique élément de $\mathbb{P}_n$. On notera $[x_0, \ldots, x_n]$ cet élément que nous appelons des coordonnées homogènes de u dans $\mathbb{P}_n$. Le choix d'un représentant de $[x_0, \ldots, x_n]$ est un choix de coordonnées homogènes pour x.*

A partir de ces définitions, on obtient directement le fait que $[x_0, \ldots, x_n] = [y_0, \ldots, y_n]$ dans $\mathbb{P}_n$ si et seulement si il existe $\lambda \in \mathbb{C}^*$ tel que $(x_0, \ldots, x_n) = (\lambda y_0, \ldots, \lambda y_n)$. Le fait que l'espace $\mathbb{P}_n$ est de dimensions n alors qu'il est construit à partir de $\mathbb{C}^{n+1}$ peut se comprendre en un sens : on a contracté les droites de $\mathbb{C}^{n+1}$ en des points, et on "perd" une dimension.

Par la suite, on va vouloir définir une topologie sur $\mathbb{P}_n$. Pour ce faire, on considère l'application $\pi : \mathbb{C}^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}_n$ qui envoie $(x_0, \ldots, x_n)$ sur $[x_0, \ldots, x_n]$. On remarque que π est en fait la projection canonique de $\mathbb{C}^{n+1} \setminus \{0\}$ dans $\mathbb{P}_n$. On définit alors la topologie de $\mathbb{P}_n$ comme étant la topologie quotient induite par l'application π, c'est à dire la topologie la plus fine rendant l'application π continue.

Remarques :

1. Par définition, U est ouvert dans $\mathbb{P}_n$ si et seulement si $\pi^{-1}(U)$ est ouvert dans $\mathbb{C}^{n+1} \setminus \{0\}$. De même, F est fermé dans $\mathbb{P}_n$ si et seulement si $\pi^{-1}(F)$ est fermé dans $\mathbb{C}^{n+1} \setminus \{0\}$.
2. Si X est un espace topologique, une application $f : \mathbb{P}_n \longrightarrow X$ est continue si et seulement si l'application $f \circ \pi : \mathbb{C}^{n+1} \setminus \{0\} \longrightarrow X$ est continue.

Nous allons maintenant étudier la topologie de $\mathbb{P}_n$. Nous allons entre-autre voir que c'est un espace séparé et qui est un espace compact, contrairement à $\mathbb{C}^n$.

On considère les ensembles

$$U_j = \{[x_0, \ldots, x_n] \in \mathbb{P}_n \mid x_j \neq 0\}$$

pour $0 \leq j \leq n$. On note que pour tout j, l'ensemble U_j est un ouvert de $\mathbb{P}_n$: $\pi^{-1}(U_j)$ est un ouvert de $\mathbb{C}^{n+1} \setminus \{0\}$, c'est l'ensemble $\{(x_0, \ldots, x_n) \in \mathbb{C}^{n+1} \setminus \{0\} \mid x_j \neq 0\}$ dont le complémentaire est un fermé de $\mathbb{C}^{n+1} \setminus \{0\}$.

Montrons que chaque U_j est homéomorphe à $\mathbb{C}^n$. Définissons l'application $\phi_j : U_j \longrightarrow \mathbb{C}^n$ donnée par

$$\phi_j([x_0,\dots,x_n]) = \left(\frac{x_0}{x_j},\dots,\frac{x_n}{x_j}\right)$$

où on aura enlevé la j-ième coordonnée. Cette application est bien définie (elle ne dépend pas que de la classe d'équivalence de $[x_0,\dots,x_n]$) et est inversible d'inverse continue

$$(y_1,\dots,y_n) \longrightarrow [y_0,\dots,y_{j-1},1,y_{j+1},\dots,y_n]$$

Les coefficients de l'image de $[x_0,\dots,x_n]$ sous l'application ϕ_j sont appelées les *coordonnées inhomogènes sur* U_j. Les fonctions ϕ_j sont continues car les $\phi_j \circ \pi : \pi^{-1}(U_j) \longrightarrow \mathbb{C}^n$ sont continues. De plus, ϕ_j est la composition de π avec la fonction continue qui à $(y_0,\dots,y_{j-1},y_{j+1},\dots,y_n)$ associe $(y_0,\dots,y_{j-1},1,y_{j+1},\dots,y_n)$. Ainsi, les ϕ_j sont des homéomorphismes.

Remarquons au passage que le complémentaire de U_n dans $\mathbb{P}_n$ est

$$V_n = \{[x_0,\dots,x_n] \in \mathbb{P}_n \mid x_n = 0\}$$

qui est naturellement identifiable à $\mathbb{P}_{n-1}$. Cela donne une intuition sur la manière de construire les espaces $\mathbb{P}_n$ par récurrence. On a $\mathbb{P}_0$ qui est un point. $\mathbb{P}_1$ est le plan complexe possédant un point "à l'infini" correspondant à $\mathbb{P}_0$. $\mathbb{P}_2$ est $\mathbb{C}^2$ possédant une droite "à l'infini" correspondant à $\mathbb{P}_1$. Cependant, on remarque aussi que l'on a, pour le cas de $\mathbb{P}_2$ une infinité de droites possible qui soient "à l'infini". En effet, $\mathbb{P}_1$ possède comme unique point à l'infini $[1,0]$. Tandis que les points à l'infini de $\mathbb{P}_2$ sont de la forme $[x,y,0]$ qui forment une droite.

Comme les ensembles U_j sont des ouverts recouvrant $\mathbb{P}_n$ et que les fonctions ϕ_j sont des homéomorphismes, une application $f : \mathbb{P}_n \longrightarrow X$ est continue si et seulement si $f \circ \phi_j^{-1}$ est continue pour tout $0 \leq j \leq n$.

Nous avons maintenant tout les outils afin d'étudier la topologie de $\mathbb{P}_n$.

Propriété 3.1.3. *$\mathbb{P}_n$ est un espace compact.*

Démonstration : Tout d'abord, rappelons que l'image d'un ensemble compact par une application continue est compact. On considère l'ensemble

$$\mathbb{S}^n = \{(x_0,\dots,x_n) \in \mathbb{C}^{n+1} \mid |x_0|^2 + \cdots + |x_n|^2 = 1\}$$

C'est un ensemble fermé et borné de $\mathbb{C}^{n+1}$, donc c'est un ensemble compact.
Puisque π est continue, il suffit donc de montrer que $\pi(\mathbb{S}^n) = \mathbb{P}_n$. Soit $[x_0,\dots,x_n] \in \mathbb{P}_n$. Si $|x_0|^2 + \cdots + |x_n|^2 = \lambda > 0$, alors

$$[x_0,\dots,x_n] = \left[\frac{x_0}{\sqrt{\lambda}},\dots,\frac{x_n}{\sqrt{\lambda}}\right]$$

Mais $|\frac{x_0}{\sqrt{\lambda}}|^2 + \cdots + |\frac{x_n}{\sqrt{\lambda}}|^2 = 1$, on en déduit donc que $[x_0,\dots,x_n] \in \pi(\mathbb{S}^n)$. On en déduit ainsi que $\pi(\mathbb{S}^n) = \mathbb{P}_n$ est compact. □

Au passage, cette démonstration nous fournit aussi que $\mathbb{P}_n$ est connexe, comme image par une application continue d'un espace connexe.

Nous allons montrer une nouvelle propriété de $\mathbb{P}_n$, à savoir que c'est un espace topologique séparé, c'est à dire que tout points distincts peuvent être séparés par des ouverts disjoints. On va avoir besoin avant cela de quelques lemmes et définitions.

Définition 3.1.4. *On appelle* transformation projective *ou* application projective *une application $f : \mathbb{P}_n \longrightarrow \mathbb{P}_n$ bijective tel qu'il existe une application linéaire $u : \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^{n+1}$, on a l'égalité $f \circ \pi = \pi \circ u$, ce qui revient à dire que $f([x_0, \dots, x_n]) = [y_0, \dots, y_n]$ où $(y_0, \dots, y_n) = u(x_0, \dots, x_n)$ pour tout $[x_0, \dots, x_n] \in \mathbb{P}_n$.*

Propriété 3.1.5. *Une transformation projective est une application continue.*

Démonstration : Soit f une transformation projective. Soit $u : \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^{n+1}$ une application linéaire telle que $f \circ \pi = \pi \circ u$. Alors $\pi \circ u$ est une application continue, donc $f \circ \pi$ est aussi continue. Mais on sait que f est continue si et seulement si $f \circ \pi$ l'est, d'où le résultat. □

Définition 3.1.6. *Un hyperplan de $\mathbb{P}_n$ est l'image par π d'un hyperplan de $\mathbb{C}^{n+1}$, privé du point 0.*

Lemme 3.1.7. *Soient $p_0, \dots, p_n, q \in \mathbb{P}_n$ tels qu'aucuns $(n+1) - uplets$ de ces éléments ne soient tous dans un même hyperplan de $\mathbb{P}_n$. Alors il existe une unique application projective qui transforme p_i en $[0, \dots, 0, \underbrace{1}_{\text{position } i}, 0, \dots, 0]$ et q en $[1, \dots, 1]$.*

Démonstration : L'idée est que l'on effectue un changement de base sur $\mathbb{P}_n$. Mais $\mathbb{P}_n$ n'a pas directement une structure d'espace vectoriel. On va donc se ramener à $\mathbb{C}^{n+1} \setminus \{0\}$.

Montrons d'abord qu'une telle application existe. Soient $u_0, \dots, u_n, v \in \mathbb{C}^{n+1} \setminus \{0\}$ des antécédents respectifs de $p_0, \dots, p_n, q$ dans $\mathbb{C}^{n+1} \setminus \{0\}$ par π. Alors $u_0, \dots, u_n$ ne sont pas nuls ni contenus tous dans le même hyperplan, sinon, on aurait $n+1$ points contenus dans le même hyperplan ce qui contredirait l'hypothèse de départ. Donc la famille $(u_i)_{0 \leq i \leq n}$ forment une base de $\mathbb{C}^{n+1}$. Ainsi, il existe une unique application linéaire α qui envoie u_i sur $(0, \dots, \underbrace{1}_{\text{position i}}, \dots, 0)$. De plus, en notant $\alpha(v) = (\lambda_0, \dots, \lambda_n)$, alors les λ_i sont non-nuls. En effet, si l'un d'eux était nul, cela voudrait dire que la i-ième composante de v serait nulle dans la base u_i et donc que $n+1$ points seraient dans le même hyperplan, ce qui contredit encore une fois l'hypothèse de départ.

Ainsi, la composition de α par l'application linéaire

$$(x_0, \dots, x_n) \longrightarrow \left(\frac{x_0}{\lambda_0}, \dots, \frac{x_n}{\lambda_n} \right)$$

définie une application projective, qui envoie p_i sur $[0, \dots, \frac{1}{\lambda_i}, \dots, 0)$ et q sur $[1, \dots, 1]$

Supposons que nous avons deux application f et f' vérifiant les hypothèses de l'énoncé. On vérifie alors que ces deux applications induisent le même changement de base dans $\mathbb{C}^{n+1}$ et ainsi elles seront égales à multiplication par un scalaire près, d'où l'unicité. □

Propriété 3.1.8. *$\mathbb{P}_n$ est un espace séparé.*

Démonstration : Soient p et q deux points disjoints de $\mathbb{P}_n$. Supposons d'abord que $p, q \in U_0$. Alors on sait que ϕ_0 est un homéomorphisme de U_0 dans $\mathbb{C}^n$, donc $\phi_0(p)$ et $\phi_0(q)$ sont disjoints. Comme $\mathbb{C}^n$ est séparé, on en déduit qu'il existe V et W deux ouverts disjoints tels que $\phi_0(p) \in V$ et $\phi_0(q) \in W$, donc $\phi_0^{-1}(V)$ et $\phi_0^{-1}(W)$ sont deux ouverts disjoints de $\mathbb{P}_n$ qui séparent p et q. En particulier, cela est vrai pour $p = [1, 0, \dots, 0]$ et $q = [1, \dots, 1]$.

Dans le cas général, prenons $p_0, \dots, p_n, q \in \mathbb{P}_n$ tels que $p_0 = p$ et tels que ces éléments vérifient les hypothèses du lemme précédent. Alors, d'après le lemme précédent, il existe f qui envoie p_0 sur $[1, 0, \dots, 0]$ et q sur $[1, \dots, 1]$. Mais donc il existe V et W deux ouverts qui séparent $f(p)$ et $f(q)$. Comme f est continue, on a $f^{-1}(V)$ et $f^{-1}(W)$ qui sont des ouverts disjoints séparant p et q. □

3.2 Courbes projectives complexes

Nous allons ici introduire les notions de bases de géométrie algébriques dont nous aurons besoin dans la suite, puis nous définirons et donnerons des propriétés des courbes projectives complexes qui nous seront utiles dans la suite. Dans toute la suite, k désignera les corps $\mathbb{R}$ ou $\mathbb{C}$.

Définition 3.2.1. *Soit $n \geq 1$ et $S \subset k[X_1, \dots, X_n]$. L'ensemble défini par $V(S) = \{x \in k^n \mid \forall P \in S,\ P(x) = 0\}$ est appelé l'ensemble algébrique affine défini par S. On peut aussi voir V comme une application qui à une partie $S \subset k[X_1, \dots, X_n]$ associe l'ensemble $V(S)$.*

Quelques remarques en vrac sur V :

1. Si $n = 1$, et si S n'est pas réduit à 0, alors $V(S)$ est un ensemble fini.
2. Si $n = 2$, alors $V(S)$ permet de définir les courbes du plan.
3. Si $S \subset S'$, alors $V(S') \subset V(S)$.

Remarquons aussi que si $S \subset k[X_1, \dots, X_n]$, notons (S) l'idéal engendré par S dans $k[X_1, \dots, X_n]$. Alors $V(S) = V((S))$ D'une part, on a $S \subset (S)$, donc $V((S)) \subset V(S)$. Réciproquement, si $x \in V(S)$ il est annulé par tout les polynômes de S, donc par tout les polynômes de (S), d'où l'inclusion réciproque. Il suffit donc d'étudier les ensembles algébriques affines qui sont définis par des idéaux. Il suffit même de se limiter aux générateurs de l'idéal puisque $k[X_1, \dots, X_n]$ est noethérien. Ainsi, si on note $I = (f_1, \dots, f_r)$, alors $V(I) = V(f_1, \dots, f_r) = V(f_1) \cap \dots \cap V(f_r)$. De plus, tout ensemble algébrique affine est une intersection de $V(f)$ où on a $f \in k[X_1, \dots, X_n]$.

Comme les polynômes sont continues, les ensembles algébriques affines sont fermés pour la topologie usuelle sur k^n. Cependant, un tel ensemble n'est pas nécessairement compact. Ainsi, on aimerait étendre la définition d'ensemble algébrique affine aux espaces projectifs. En effet, cela permettra de rendre les courbes compactes.

Cependant, un problème se pose. En effet, comme un point de $\mathbb{P}_n$ est une classe d'équivalence de points, l'évaluation d'un polynôme est impossible. On peut cependant contourner cette difficulté dans $\mathbb{C}$ en considérant des polynômes homogènes. On dira qu'un polynôme de $k[X_1, \dots, X_n]$ s'annule en un point $x \in \mathbb{P}_n$ si et seulement si il s'annule pour tout système de coordonnées homogènes de x.

Définition 3.2.2. *Soit $n \geq 1$ et $P \in k[X_1, \dots, X_n]$. On dit que P est un* polynôme homogène *de degré d si $\forall \lambda \in k$, $P(\lambda X_1, \dots, \lambda X_k) = \lambda^d P(X_1, \dots, X_n)$.*

Définition 3.2.3. *Soit $P \in k[X_1, \dots, X_n]$ et $x \in \mathbb{P}_n$. On dira que x est un zéro de P si P s'annule sur tout les systèmes de coordonnées homogènes associés à x. On continuera de noter cela $P(x) = 0$. De plus, si P est homogène, il suffit que $P(x) = 0$ pour un seul système de coordonné.*

On a maintenant le bon cadre pour définir les ensembles algébriques projectifs.

Définition 3.2.4. *Soit $S \subset k[X_0, \dots, X_n]$ un sous-ensemble de polynômes homogènes. On appelle* ensemble algébrique projectif définit par S *l'ensemble $V_p(S) = \{x \in \mathbb{P}_n \mid \forall P \in S, P(x) = 0\}$.*

Comme dans le cas affine, du fait que $k[X_1, \ldots, X_n]$ est noethérien, on peut se ramener au cas où S est fini. En fait, on peut même se ramener au cas où S est fini et où tout les polynômes sont homogènes.

Nous sommes maintenant armés afin de pouvoir proprement définir une courbe projective sur l'ensemble $\mathbb{P}_2$. Rappelons que ce dernier espace est construit comme étant l'espace projectif associé à $\mathbb{C}^3$.

Définition 3.2.5. *Soit $P \in \mathbb{C}[X, Y, Z]$ un polynôme homogène non-constant. On définit la* courbe projective complexe $\mathcal{C}$ associée à P *comme étant l'ensemble*

$$\mathcal{C} = \{[x, y, z] \in \mathbb{P}_2 \mid P(x, y, z) = 0\}$$

L'égalité est ici à comprendre au sens définit précédemment dans la partie 1.2.2.

À partir de cette définition, nous allons introduire différentes notations :

1. Le degré de la courbe projective complexe $\mathcal{C}$ associée au polynôme homogène P est le degré du polynôme P.
2. La courbe projective complexe $\mathcal{C}$ est dite irréductible si son polynôme minimal associé est irréductible.
3. Une courbe projective complexe irréductible $\mathcal{D}$ est une composante de la courbe projective complexe $\mathcal{C}$ si le polynôme minimal associé à $\mathcal{D}$ divise le polynôme minimal associé à $\mathcal{C}$.

On souhaite que la courbe projective complexe soit localement une sous-variété complexe. Pour cela, il faut ajouter une hypothèse de régularité sur la courbe, ce qui motive la définition suivante.

Définition 3.2.6. *Soit $\mathcal{C}$ une courbe projective complexe de $\mathbb{P}_2$ et soit P son polynôme minimal associé. On dit que $[a, b, c] \in \mathcal{C}$ est un point singulier si*

$$\frac{\partial P}{\partial x}[a, b, c] = \frac{\partial P}{\partial y}[a, b, c] = \frac{\partial P}{\partial z}[a, b, c] = 0$$

L'ensemble des points singuliers de $\mathcal{C}$ est noté $\mathrm{Sing}(\mathcal{C})$. La courbe est dite non-singulière si $\mathrm{Sing}\,(\mathcal{C}) = \emptyset$.

Remarquons que si $\mathcal{C}$ est une courbe projective complexe, si $p \notin \mathrm{Sing}\,(\mathcal{C})$, alors $\mathcal{C}$ est une sous-variété complexe de $\mathbb{P}_2$ dans un voisinage de p. Cet énoncé est loin d'être immédiat et va être démontré dans la suite.

Exemples :

1. Soit $P(x, y, z) = x^2 + y^2 - z^2$. On voit que P définit bien une courbe $\mathcal{C}$ sur $\mathbb{P}_2$. De plus, on a :

$$\frac{\partial P}{\partial x} = 2x, \ \frac{\partial P}{\partial y} = 2y, \ \frac{\partial P}{\partial z} = -2z$$

   Ces expressions sont toutes nulles en même temps dans $\mathbb{C}^3$ si et seulement si $(x, y, z) = (0, 0, 0)$. Mais $(0, 0, 0)$ n'a pas d'image dans $\mathbb{P}_2$, on en déduit donc que $\mathcal{C}$ est non-singulière.
2. Soit $P(x, y, z) = y^2 z - x^3$. P définit bien une courbe projective complexe $\mathcal{C}$. On a :

$$\frac{\partial P}{\partial x} = -3x^2, \ \frac{\partial P}{\partial y} = 2zy, \ \frac{\partial P}{\partial x} = y^2$$

   Ces trois expressions s'annulent en même temps au point $(0, 0, 1)$, dont l'image dans $\mathbb{P}_2$ est $[0, 0, 1]$. On en déduit donc que $\mathcal{C}$ est singulière.

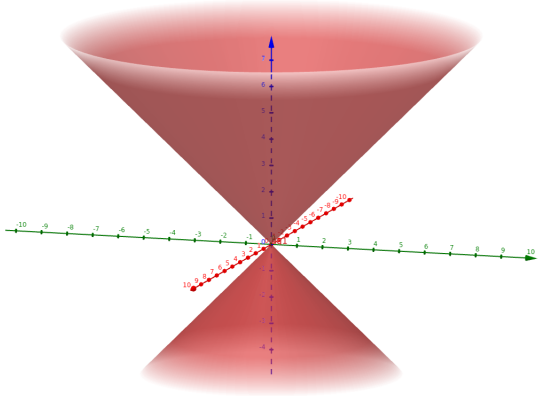

FIGURE 4 – *La courbe définie dans l'exemple 1 dans* $\mathbb{R}$. *On voit que* $(0,0,0)$ *est un point singulier qui n'est pas présent sur la courbe projective.*

On va maintenant s'intéresser à une classe particulière de courbes projectives complexes, à savoir les cubiques.

Définition 3.2.7. *Une cubique de* $\mathbb{P}_2$ *est une courbe projective complexe dont le polynôme homogène associé est de degré 3.*

Avant de continuer, on énonce une propriété des cubiques de $\mathbb{P}_2$ non-singulières. Nous ne démontrerons pas ccette propriété, dont une démonstration peut se trouver dans [1] p.73.

Propriété 3.2.8. *Soit* $\mathcal{C}$ *une cubique de* $\mathbb{P}_2$. *Si* $\mathcal{C}$ *n'est pas singulière, alors elle est équivalente à une courbe définie par un polynôme de la forme*

$$y^2z = (x - az)(x - bz)(x - cz)$$

avec a, b, c *des nombres complexes distincts.*

Nous allons maintenant démontrer un lemme sur les polynômes homogènes qui nous permettra entre-autre de démontrer qu'une courbe projective complexe non-singulière $\mathcal{C}$ est une surface de Riemann.

Lemme 3.2.9. *Soit* $P(x, y, z)$ *un polynôme homogène de degré* d. *Alors* P *vérifie*

$$x\frac{\partial P}{\partial x}(x,y,z) + y\frac{\partial P}{\partial y}(x,y,z) + z\frac{\partial P}{\partial z}(x,y,z) = dP(x,y,z)$$

Soit $\lambda \in \mathbb{C}$. la fonction $\lambda \longrightarrow P(\lambda x, \lambda y, \lambda z)$ est dérivable et on a

$$\frac{\partial P(\lambda x, \lambda y, \lambda z)}{\partial \lambda} = \frac{\partial P}{\partial x}(\lambda x, \lambda y, \lambda z) + y\frac{\partial P}{\partial y}(\lambda x, \lambda y, \lambda z) + z\frac{\partial P}{\partial z}(\lambda x, \lambda y, \lambda z)$$

Mais on sait aussi que P est homogène donc on a aussi que

$$\frac{\partial P(\lambda x, \lambda y, \lambda z)}{\partial \lambda} = d\lambda^{d-1}P(x,y,z)$$

et il suffit donc d'évaluer cette expression en $\lambda = 1$. □

On va maintenant montrer un résultat qui nous sera fondamental dans la suite de cette partie, à savoir qu'une cubique de $\mathbb{P}_2$ possède une structure de surface de Riemann. On montrera en fait un résultat un peu plus général, qui est que toute courbe projective sur $\mathbb{P}_2$ possède une structure de surface de Riemann, sauf en les singularités de la courbe.

Théorème 3.2.10. *Soit $\mathcal{C}$ une courbe projective de $\mathbb{P}_2$ définie par le polynôme homogène $P(X,Y,Z)$ de degré d et soit S l'ensemble de ses singularités. Alors $\mathcal{C} \setminus S$ est une surface de Riemann.*

Démonstration : On considère $[a,b,c] \in \mathcal{C}$, c'est à dire que $P(a,b,c) = 0$. Supposons dans un premier temps que $\frac{\partial P}{\partial y}(a,b,c) \neq 0$. Par le lemme 1.3.5, on sait que

$$a\frac{\partial P}{\partial x}(a,b,c) + b\frac{\partial P}{\partial y}(a,b,c) + c\frac{\partial P}{\partial z}(a,b,c) = 0$$

Si on a $a = c = 0$, on en déduit que $b = 0$, ce qui est impossible car $(0,0,0)$ n'a pas d'image dans $\mathbb{P}_2$. Ainsi, on a $a \neq 0$ ou $c \neq 0$.

Supposons ici que $c \neq 0$. Comme P est homogène de degré d, on a

$$\frac{\partial P}{\partial y}\left(\frac{a}{c}, \frac{b}{c}, 1\right) = \frac{1}{c^{d-1}}\frac{\partial P}{\partial y}(a,b,c) \neq 0$$

Par le théorème des fonctions implicites holomorphe, il existe V un voisinage de $\frac{a}{c}$ dans $\mathbb{C}$, W un voisinage de $\frac{b}{c}$ dans $\mathbb{C}$ et une fonction $g : V \longrightarrow W$ holomorphe tels que pour tout $x \in V$ et pour tout $y \in W$,

$$P(x,y,1) = 0 \;\Leftrightarrow\; g(x) = y$$

Quitte à restreindre V et W, on définit U l'ouvert de $\mathcal{C} \setminus S$ par

$$\begin{aligned} U &= \left\{ [x,y,z] \in \mathcal{C} \mid z \neq 0,\ \frac{x}{z} \in V,\ \frac{y}{z} \in W \right\} \\ &= \{ [x,y,1] \in \mathcal{C} \mid x \in V,\ y \in W \} \end{aligned}$$

Ainsi, la fonction $\phi : U \longrightarrow V$ définit par

$$\phi[x,y,z] = \frac{x}{z}$$

est un homéomorphisme d'inverse $w \longrightarrow [w, g(w), 1]$.

De manière similaire, on traite les cas où $a \neq 0$, $\frac{\partial P}{\partial x}(a,b,c) \neq 0$, $\frac{\partial P}{\partial z}(a,b,c) \neq 0$. C'est à dire que dans tout voisinage de chaque point de $\mathcal{C} \setminus S$, l'on peut trouver un ouvert U de $\mathcal{C} \setminus S$, un ouvert V de $\mathbb{C}$ et un homéomorphisme $\phi : U \longrightarrow V$ de sorte que $\phi[x,y,z]$ soit l'une des valeurs suivantes :

$$\frac{z}{x}, \frac{y}{z}, \frac{z}{y}, \frac{x}{y}, \frac{y}{x}$$

et un inverse de la forme $w \longrightarrow [1, g(w), w]$, $[g(w), w, 1]$, $[g(w), 1, w]$, $[w, 1, g(w)]$ ou $[1, w, g(w)]$, avec $g : V \longrightarrow \mathbb{C}$ holomorphe. On obtient ainsi un atlas (U_i, ϕ_i) de $\mathcal{C} \setminus S$. Or, les fonctions

$$w \longrightarrow w,\ \frac{1}{w},\ g(w),\ \frac{1}{g(w)},\ \frac{w}{g(w)},\ \frac{g(w)}{w}$$

sont biens définies et holomorphes aux voisinages des ouverts où elles sont définies. Ainsi, on en déduit de (U_i, ϕ_i) est un atlas holomorphe de $\mathcal{C} \setminus S$. □

La dernière chose qu'il nous faut faire dans cette partie est de définir ce qu'est un point de ramification d'une fonction sur une courbe projective complexe $\mathcal{C}$ afin de pouvoir mieux appréhender la topologie des courbes projectives complexes.

Commençons par un exemple. On considère la courbe $\mathcal{C}$ donnée par l'équation $y^2 = xz$. On considère la fonction $\phi : \mathcal{C} \longrightarrow \mathbb{P}_1$ donnée par

$$\phi[x, y, z] = [x, z]$$

On voit que ϕ est une fonction surjective. De plus, si $x \neq 0$ et $z \neq 0$, on a

$$\phi^{-1} = \{[x, y_1, z], [x, y_2, z]\}$$

où y_1 et y_2 sont les deux racines carrées de xz. Dans l'autre cas, $[0, 1]$ et $[1, 0]$ ont un unique antécédent par ϕ.

Soit $\mathcal{C}$ une courbe projective complexe non singulière définie par le polynôme homogène P de degré $d > 1$. Quitte à changer les coordonnées en appliquant une transformation projective, on peut supposer que $[0, 1, 0] \notin \mathcal{C}$. Ainsi, l'application $\phi : \mathcal{C} \longrightarrow \mathbb{P}_1$ définie par

$$\phi[x, y, z] = [x, z]$$

est bien définie.

Définition 3.2.11. *On appelle indice de ramification $\nu_\phi[a, b, c]$ de la fonction ϕ au point $[a, b, c] \in \mathcal{C}$ l'ordre du zéro du polynôme en y $P(a, y, c)$ au point $y = b$. Le point $[a, b, c]$ est appelé point de ramification de ϕ si $\nu_\phi[a, b, c] > 1$.*

Remarques :

1. On a $\nu_\phi[a, b, c] > 0$ si et seulement si $[a, b, c] \in \mathcal{C}$.
2. On a $\nu_\phi[a, b, c] > 1$ si et seulement si

$$P(a, b, c) = \frac{\partial P}{\partial y}(a, b, c) = 0$$

ce qui est équivalent au fait que $[a, b, c] \in \mathcal{C}$ et que la tangente à $\mathcal{C}$ au point $[a, b, c]$ contient le point $[0, 1, 0]$.

Pour la suite, nous aurons besoin d'une version faible du théorème de Bézout et de l'un de ses corollaire. On renvoie à [1], page 54 et page 66, afin d'avoir une démonstration de ce théorème et de son corollaire.

Théorème 3.2.12 (Forme faible du théorème de Bézout). *Soient $\mathcal{C}$ et $\mathcal{D}$ deux courbes projectives complexes de $\mathbb{P}_2$ de degré m et n. Si $\mathcal{C}$ et $\mathcal{D}$ n'ont aucune composante commune, alors elles ont au plus mn points d'intersection.*

Corollaire 3.2.13. *Soient $\mathcal{C}$ et $\mathcal{D}$ deux courbes projectives complexes de degré n et m. Supposons que pour tout $p \in \mathcal{C} \cap \mathcal{D}$, p est un point non-singulier de $\mathcal{C}$ et de $\mathcal{D}$ et que les tangentes en p de $\mathcal{C}$ et de $\mathcal{D}$ sont distinctes. Alors il y a exactement nm points dans $\mathcal{C} \cap \mathcal{D}$.*

Nous allons maintenant démontrer deux lemmes qui nous seront utiles dans la preuve du théorème de Riemann-Roch en partie 4.3.

Lemme 3.2.14. *Soit $\mathcal{C}$ une courbe projective complexe non-singulière et irréductible définie par un polynôme homogène P de degré d. Soit $\phi : \mathcal{C} \longrightarrow \mathbb{P}_1$ la ramification donnée par*

$$\phi[x, y, z] = [x, z]$$

On a alors les propriétés suivantes :

1. *ϕ a au plus $d(d-1)$ points de ramification.*
2. *Si $\nu_\phi[a, b, c] \leq 2$ pour tout $[a, b, c] \in \mathcal{C}$, alors $\mathcal{C}$ a exactement $d(d-1)$ points de ramification.*

Démonstration : Par hypothèse, on a que $[0, 1, 0] \notin \mathcal{C}$. Ainsi, le coefficient de y^d de P est non-nul. Ainsi, le polynôme irréductible $\frac{\partial P}{\partial y}$ est non-nul et est de degré $d-1$ et il ne peut donc être divisible par P. Ainsi, la courbe $\mathcal{D}$ définie par le polynôme $\frac{\partial P}{\partial y}$ n'a aucune composante en commun avec $\mathcal{C}$. Par le théorème 3.2.12, ces deux courbes ont au plus $d(d-1$ points d'intersection. Ainsi, on en déduit directement que $\mathcal{C}$ a au plus $d(d-1)$ points de ramification.

Supposons que $\nu_\phi[a, b, c] \leq 2$ pour tout $[a, b, c] \in \mathcal{C}$. D'après le corollaire 3.2.13, il suffit de montrer que si $p \in \mathcal{C} \cap \mathcal{D}$, alors p n'est pas un point singulier de $\mathcal{D}$ et que la tangente en p des courbes $\mathcal{C}$ et $\mathcal{D}$ sont distinctes.

Supposons par l'absurde que les deux tangentes sont identiques. Alors un tel $[a, b, c] \in \mathcal{C} \cap \mathcal{D}$ vérifie

$$P[a, b, c] = \frac{\partial P}{\partial y}[a, b, c] = 0$$

De plus, $[a, b, c]$ est dans la tangente à $\mathcal{D}$, qui est la même que la tangente à $\mathcal{C}$, donc $[a, b, c]$ vérifie que la quantité

$$\left(\frac{\partial^2 P}{\partial x \partial y}[a, b, c], \frac{\partial^2 P}{\partial y^2}[a, b, c], \frac{\partial^2 P}{\partial z \partial y}[a, b, c]\right)$$

est soit nulle, soit un multiple de

$$\left(\frac{\partial P}{\partial x}[a, b, c], \frac{\partial P}{\partial y}[a, b, c], \frac{\partial P}{\partial z}[a, b, c]\right)$$

Dans tout les cas, cela implique que

$$P[a, b, c] = \frac{\partial P}{\partial y}[a, b, c] = \frac{\partial^2 P}{\partial y^2}[a, b, c] = 0$$

ce qui contredit le fait que $\nu_\phi[a, b, c] \leq 2$. □

Nous admettrons le lemme suivant, dont une démonstration peut être trouvée dans [1], page 98.

Lemme 3.2.15. *Soit $\mathcal{C}$ une courbe projective complexe non-singulière. En appliquant une transformation projective adéquate, on a*

$$\nu_\phi[a,b,c] \leq 2$$

et ce pour tout $[a,b,c] \in \mathcal{C}$.

3.3 Paramétrisation des cubiques de $\mathbb{P}_2$ par les fonctions de Weierstrass

Dans cette partie, nous allons montrer que les tores complexes sont biholomorphes à des cubiques définies sur $\mathbb{P}_2$ et donc que les tores complexes sont exactement les courbes elliptiques.

Définition 3.3.1. *Soit Λ un réseau et g_2, g_3 les fonctions défini à la proposition 2.2.3. On définit la cubique $\mathcal{C}_\Lambda$ comme étant le lieu d'annulation du polynôme homogène :*

$$Q(x,y,z) = y^2z - 4x^3 + g_2xz^2 + g_3z^3$$

Propriété 3.3.2. *La cubique $\mathcal{C}_\Lambda$ est non-singulière.*

Démonstration : D'après la propriété 3.2.8, il suffit de montrer qu'il existe a, b, c trois complexes distincts tels que

$$y^2z = 4(x-az)(x-bz)(x-cz)$$

Soit $\wp$ la fonction de Weierstrass associée au réseau Λ. On considère les quantités $a = \wp(\frac{\omega_1}{2})$, $b = \wp(\frac{\omega_2}{2})$ et $c = \wp(\frac{\omega_1+\omega_2}{2})$. Par la proposition 2.1.6, ces trois nombres sont distincts et, de la même manière que dans la preuve de la proposition 2.1.6, on a $\wp'(\frac{\omega_1}{2}) = 0$ (de même pour les autres).

Mais on sait que $\wp'(z)^2 = \wp(z)^3 - g_2\wp(z) - g_3$. Ainsi, a est racine du polynôme $4x^3 - g_2x - g_3$. On montre aussi que b et c sont racines de ce polynôme. On en déduit donc que az, bz et cz sont racines du polynôme $4x^3 - g_2xz^2 - g_3z^3$. Ainsi, on a que $y^2z = 4(x-az)(x-bz)(x-cz)$. □

Intéressons-nous maintenant de plus près à Λ. L'ensemble $\mathbb{C}/\Lambda$ possède une structure de groupe quotient, dont les éléments sont de la forme $[\Lambda + z]$ avec $z \in \mathbb{C}$. On note π la projection canonique. De plus, ce groupe possède aussi une topologie quotient induite par celle de $\mathbb{C}$. On a donc que U est un ouvert de $\mathbb{C}/\Lambda$ si et seulement si $\pi^{-1}(U)$ est un ouvert de $\mathbb{C}$.

L'application π est une application ouverte. En effet, si U est un ouvert de $\mathbb{C}$, l'égalité $\pi^{-1}(\pi(U)) = \bigcup_{\omega\in\Lambda}(U+\omega)$ nous donne directement que $\pi(U)$ est un ouvert.

Topologiquement, $\mathbb{C}/\Lambda$ est un tore. En effet, en partant du parallélogramme de points 0, ω_1, ω_2 et $\omega_1+\omega_2$, que l'on a identifié les bords des deux côtés. On appelle cette objet un *tore complexe*. On va maintenant pouvoir montrer que toute cubique non-singulière sur $\mathbb{P}_2$ est un tore complexe.

Théorème 3.3.3. *Soit Λ un réseau de $\mathbb{C}$ et $\wp$ sa fonction de Weierstrass associée. On définit l'application $u : \mathbb{C}/\Lambda \longrightarrow \mathcal{C}_\Lambda$ définie par*

$$u(\Lambda+z) = \begin{cases} [\wp(z), \wp'(z), 1] & si \quad z \notin \Lambda \\ [0,1,0] & si \quad z \in \Lambda \end{cases}$$

Alors u est bien définie est un homéomorphisme sur son image.

Démonstration : Dans un premier temps, montrons que u est bien définie.

Si $\Lambda + z = \Lambda + w$, alors de part la double périodicité de $\wp$, on a bien que $u(\Lambda + z) = u(\Lambda + w)$. De plus, on sait que $\wp'(z)^2 = 4\wp^3(z) - g_2\wp(z) - g_3$, donc $[\wp(z), \wp'(z), 1] \in \mathcal{C}_\Lambda$. Ainsi, u est bien définie.

Montrons que u est injective. Soient $z, w \in \mathbb{C} \setminus \Lambda$ et supposons que l'on a $u(\Lambda + z) = u(\Lambda + w)$. Alors $\wp(z) = \wp(w)$. On a alors que $z \in \pm w$. Si $z \in \Lambda + w$, alors on aura l'injectivité.

Supposons alors que $z \in \Lambda - w$. Comme $\wp'$ est doublement périodique et est impaire, on a $\wp'(z) = \wp'(-w) = -\wp'(w)$. Mais on a aussi que $u(z) = u(w)$ donc $\wp'(z) = 0$. Donc, en reprenant la preuve de la propriété 2.1.6, on a $\wp \in \{a, b, c\}$. On a, par surjectivité, que $w \in \frac{1}{2}\Lambda$ et donc que $w - \Lambda = w + \Lambda$. Ainsi, u est bien injective.

Montrons que u est surjective. Soit $[\alpha, \beta, \gamma] \in \mathcal{C}_\Lambda$. Si $\gamma = 0$, d'après l'équation qui définie $\mathcal{C}_\Lambda$, on a que $\alpha = 0$ et ainsi $[\alpha, \beta, \gamma] = [0, 1, 0]$, qui est bien dans l'image de u.

Supposons donc, sans perte de généralité, que $\gamma \neq 1$. Par surjectivité de $\wp$, il existe $z \in \mathbb{C}$ tel que $\wp(z) = \alpha$. Mais alors, $\wp'(z)^2 = 4\alpha^3 - g_2\alpha - g_3 = \beta^2$. Donc $\wp'(z) = \pm\beta$. Si $\wp'(z) = \beta$, alors on a bien $[\alpha, \beta, 1]$ qu'est dans l'image de u. Si $\wp'(z) = -\beta$, alors par imparité de $\wp'$, on a que $\wp'(-z) = \beta$, et aussi que $\wp(-z) = \wp(z) = \alpha$ par parité de $\wp$, et on a donc $[\alpha, \beta, 1]$ qu'est dans l'image de u. Ainsi, u est bien surjective, et donc elle est bien bijective.

Comme $\wp$ et $\wp'$ sont continues sur $\mathbb{C} \setminus \Lambda$, alors u est continue sur $\mathbb{C}/\Lambda \setminus \{\Lambda + 0\}$. Au voisinage de 0, on a $\wp(z) = \frac{g(z)}{z^2}$ et $\wp'(z) = \frac{h(z)}{z^3}$ avec g et h des fonctions holomorphes bornées au voisinage de 0 et ne s'annulant pas en 0. Pour z proche de 0, on a alors

$$u(\Lambda + z) = [\wp(z), \wp'(z), 1] = [zg(z), h(z), z^3]$$

qui tend vers $[0, 1, 0]$ quand z tend vers 0. Ainsi, u est bien continue partout. De plus, on sait que $\mathcal{C}_\Lambda$ est un sous-espace fermé d'un espace compact, donc il est séparé. De plus $\mathbb{C}/\Lambda$ est compact. Ainsi, on en déduit que u est une application fermée, et donc que c'est un homéomorphisme. □

On va maintenant montrer que cet homéomorphisme est en réalité un biholomorphisme.

Théorème 3.3.4. *L'homéomorphisme*

$$u(\Lambda + z) = \begin{cases} [\wp(z), \wp'(z), 1] & \text{si} \quad z \notin \Lambda \\ [0, 1, 0] & \text{si} \quad z \in \Lambda \end{cases}$$

défini au théorème 3.3.3 est un biholomorphisme.

Démonstration : On considère un tore $\mathbb{C}/\Lambda$ munit de l'atlas holomorphe défini comme dans la démonstration du théorème 1.1.2. On considère de même la courbe projective complexe $\mathcal{C}_\Lambda$ associée au réseau, munit de l'atlas holomorphe défini comme dans la démonstration du théorème 3.2.10.

On notera $\varphi_i : U_i \longrightarrow V_i$ et $\psi_j : W_j \longrightarrow Y_j$ les applications de cartes de $\mathbb{C}/\Lambda$ et de $\mathcal{C}_\Lambda$. On veut montrer que l'application

$$\psi_j \circ u \circ \varphi_i^{-1} : \varphi_i(U_i \cap u^{-1}(W_j)) \longrightarrow Y_j$$

est une application holomorphe. En effet, on aura ainsi une application holomorphe bijective, donc son inverse sera automatiquement holomorphe. Par la démonstration du théorème 1.1.2, on sait que l'on peut prendre φ_i comme étant l'inverse de

$$\pi : V_i \longrightarrow U_i$$

où V_i est un disque ouvert suffisamment petit et $\pi : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda$ est la projection canonique.

Si $w \notin \Lambda$, alors $u(w + \Lambda) = [\wp(w), \wp'(w), 1]$ et par la preuve du théorème 1.3.6, on sait que ψ_j est de la forme

$$[x, y, z] \mapsto \frac{x}{z}$$
$$[x, y, z] \mapsto \frac{y}{z}$$

et ainsi $\psi_j \circ u \circ \varphi_i^{-1}$ est la restriction de $\wp$ ou de $\wp'$ qui est bien une fonction holomorphe.

Si $w \in \Lambda$, en notant Q_Λ le polynôme homogène associé à la courbe $\mathcal{C}_\Lambda$ (c.f la définition 3.3.1), la démonstration du théorème 3.2.10 et le fait que

$$\frac{\partial Q_\Lambda}{\partial z}(0, 1, 0) \neq 0$$

nous donne que

$$\psi_j \circ u \circ \varphi_i(z) = \begin{cases} \frac{\wp(z)}{\wp'(z)} \text{ si } z \notin \Lambda \\ 0 \text{ si } z \in \Lambda \end{cases}$$

Mais, au voisinage de w, $\wp$ possède un pôle d'ordre 2 et $\wp'$ un pôle d'ordre 3. Donc $\frac{\wp(z)}{\wp'(z)}$ est bien défini et est holomorphe au voisinage de w, et donc $\psi_j \circ u \circ \varphi_i$ est bien holomorphe dans ce cas. □

Ainsi, chaque tore complexe est envoyé sur une courbe elliptique. Pour la réciproque, il nous faut introduire l'intégration sur une surface de Riemann, qui est l'un des buts de la partie 4 de ce dossier. Cette réciproque ne sera pas démontrée ici. On peut retrouver la démonstration sous la forme d'un exercice dans [1], page 181.

4 Intégration sur une surface de Riemann et théorème de Riemann-Roch

Le but de cette section est double. Tout d'abord, étant donné un réseau Λ de $\mathbb{C}$, on peut retrouver, à l'aide du biholomorphisme u définit en 3.3.4, la courbe elliptique associée. Quand est-il du problème inverse ? Étant donné une courbe elliptique, est-il possible de retrouver le réseau Λ qui la caractérise ? Cette question revient à expliciter u^{-1}. Nous aurons besoin pour cela de la théorie de l'intégration sur une surface de Riemann.

Le deuxième but de cette section est de démontrer le théorème de Riemann-Roch. On sait qu'une courbe elliptique est le quotient d'un tore par un réseau. Cela fournit ainsi à la courbe elliptique une structure naturelle de groupe. Cependant, il est possible de donner une structure de groupe à la courbe elliptique sans passer par cette description de la courbe et qui a un intérêt en soi. Le théorème de Riemann-Roch permet de mettre en lumière cette structure de groupe sur une courbe elliptique.

4.1 Différentielle holomorphe et intégration sur les surfaces de Riemann

Dans cette section, nous allons introduire les outils nécessaire afin de pouvoir définir une intégrale sur une surface de Riemann quelconque. Si rien n'est précisé, $\mathcal{C}$ définira une courbe complexe projective sur $\mathbb{P}_2$.

De la même manière que dans le cas de $\mathbb{C}$, nous allons intégrer sur des chemins. Il faut donc définir la notion de chemin sur une surface de Riemann.

Définition 4.1.1. *Soit $[a,b] \subset \mathbb{R}$ un intervalle et X une surface de Riemann. Un chemin $\mathcal{C}^1$ par morceau (ou juste chemin) γ de X est une application continue $\gamma : [a,b] \longrightarrow X$ telle que si $\phi : U \longrightarrow V$ est une carte de X, et si $[c,d] \subset \gamma^{-1}(U)$, alors*

$$\phi \circ \gamma : [c,d] \longrightarrow V$$

est un chemin $\mathcal{C}^1$ par morceau de $V \subset \mathbb{C}$. On dire que γ est un lacet de X si $\gamma(a) = \gamma(b)$.

On va maintenant définir la différentielle méromorphe, qui nous permettra de définir la différentielle holomorphe afin de pouvoir intégrer sur des surfaces de Riemann.

Définition 4.1.2. *Soit X une surface de Riemann munit d'un atlas $\phi_a : U_a \longrightarrow V_a$ indexé sur un ensemble A. Une différentielle méromorphe η est une collection de fonctions méromorphes*

$$\{\eta_a : V_a \longrightarrow \mathbb{C} \cup \{\infty\}\}$$

telle que si $a, b \in A$ et $u \in U_a \cap U_b$, alors

$$\eta_a(\phi_a(u)) = \eta_b(\phi_b(u))(\phi_b \circ \phi_a^{-1})'(\phi_a(u))$$

Si f et g sont deux fonctions méromorphes sur X, on peut définir une différentielle holomorphe $\eta = f\,dg$ en posant

$$\eta_a = (f \circ \phi_a^{-1})(g \circ \phi_a^{-1})'$$

La chose a plus importante à comprendre ici est qu'une différentielle méromorphe fdg est entièrement représentée par les fonctions méromorphes.

$$(f \circ \phi^{-1})(z)(g \circ \phi^{-1})'(z)$$

Considérons η et ζ deux différentielles méromorphes. Alors $\frac{\eta_a}{\zeta_a}$ définit une fonction méromorphe indépendante du choix de a. En effet, on va avoir directement par définition que pour tout $u \in U_a$, on a

$$\frac{\eta_a(\phi_a(u))}{\zeta_a(\phi_a(u))} = \frac{\eta_b(\phi_b(u))}{\zeta_b(\phi_b(u))}$$

et donc, en posant f cette fonction méromorphe, on en déduit que $\eta = f\zeta$. Cette remarque sera importante dans la partie sur le théorème de Riemann-Roch.

Afin de pouvoir faire de l'intégration, il nous faut considérer le concept de différentielle holomorphe.

Définition 4.1.3. *Soit fdg une différentielle méromorphe. On dit que fdg est une différentielle holomorphe si les fonctions $(f \circ \phi^{-1})(z)(g \circ \phi^{-1})'(z)$ ne possèdent pas de pôles.*

Cette définition est indépendante du système de carté considéré. L'idée à avoir derrière le concept de différentielle holomorphe est qu'on regarde f dans un système de coordonnées donné par g, dans un sens qui sera précisé par la suite.

On peut maintenant définir une intégrale sur une surface de Riemann.

Définition 4.1.4. *Soit fdg une différentielle holomorphe et soit $\gamma : [a, b] \longrightarrow X$ un chemin $\mathcal{C}^1$ par morceau de X. On définit l'intégrale de fdg le long du chemin γ comme étant*

$$\int_\gamma fdg = \int_a^b (f \circ \gamma)(t)(g \circ \gamma)'(t)dt$$

Afin que cette définition ait du sens, il faut vérifier qu'elle ne dépende pas du représentant choisi, c'est à dire que si $fdg = \tilde{f}d\tilde{g}$, alors

$$\int_a^b (f \circ \gamma)(t)(g \circ \gamma)'(t)dt = \int_a^b (\tilde{f} \circ \gamma)(t)(\tilde{g} \circ \gamma)'(t)dt$$

Soit ϕ_a une carte de X. Comme on sait que $fdg = \tilde{f}d\tilde{g}$, on a que

$$(f \circ \phi_a^{-1})(g \circ \phi_a^{-1})' = (\tilde{f} \circ \phi_a^{-1})(\tilde{g} \circ \phi_a^{-1})'$$

et ce pour toute carte $\phi_a : U_a \longrightarrow V_a$ de X. De ce fait, il existe des réels

$$a = a_0 < \cdots < a_p = b$$

et des indices $\alpha_1, \ldots, \alpha_p$ qui vérifient

$$\gamma([a_{i-1}, a_i]) \subset U_{\alpha_i}$$

Ainsi, si $1 \leq i \leq p$, on a

$$\begin{aligned}\int_\gamma f dg &= \sum_{i=1}^{p} \int_{a_{i-1}}^{a_i} (f \circ \gamma)(t)(g \circ \gamma)'(t)dt \\ &= \sum_{i=1}^{p} \int_{a_{i-1}}^{a_i} (f \circ \phi_{a_i}^{-1}) \circ (\phi_{a_i} \circ \gamma)(t)(g \circ \phi_{a_i}^{-1})' \circ (\phi_{a_i} \circ \gamma)(t)(\phi_{a_i} \circ \gamma)'(t)dt\end{aligned}$$

De même, on peut faire la même chose en partant de $\int_\gamma \tilde{f} d\tilde{g}$ et obtenir ainsi la même expression que précédemment. L'intégrale ne dépend donc pas du choix du représentant de la différentielle holomorphe.

Remarquons que si $\psi : [c, d] \longrightarrow [a, b]$ est une application $\mathcal{C}^1$ par morceau, alors $\gamma \circ \psi : [c, d] \longrightarrow X$ est un chemin de X. On a donc, en effectuant le changement de variable $t = \psi(s)$ que

$$\begin{aligned}\int_\gamma f dg &= \int_a^b (f \circ \gamma)(t)(g \circ \gamma)'(t)dt \\ &= \int_c^d (f \circ \gamma \circ \psi)(s)(g \circ \gamma)'(\psi(s))\psi'(s)ds \\ &= \int_c^d (f \circ \gamma \circ \psi)(s)(g \circ \gamma \circ \psi)'(s)ds \\ &= \int_{\gamma\circ\psi} f dg\end{aligned}$$

Ainsi, l'intégrale de fdg ne dépend pas de la paramétrisation de γ choisi. On retrouve un résultat similaire à ce que l'on connaît sur $\mathbb{C}$.

Définition 4.1.5. *Soient X et Y des surfaces de Riemann et $\psi : X \longrightarrow Y$ une fonction holomorphe. Soit fdg une différentielle holomorphe sur Y. On définit une différentielle holomorphe $\psi^*(fdg)$ sur X par*

$$\psi^*(fdg) = (f \circ \psi)d(g \circ \psi)$$

La définition a bien du sens car $f \circ \psi$ et $g \circ \psi$ sont bien des fonctions holomorphes sur X.

De cette façon, étant donné fdg une différentielle holomorphe sur Y et $\psi : X \longrightarrow Y$, on peut calculer l'intégrale le long d'un chemin γ (de X) de $\psi^*(fdg)$ de la façon suivante

$$\int_\gamma \psi^*(fdg) = \int_a^b (f \circ \psi \circ \gamma)(t)(g \circ \psi \circ \gamma)'(t)dt = \int_{\psi\circ\gamma} f dg$$

On considère $\mathcal{C}$ une courbe projective complexe irréductible qui n'est pas réduite à la ligne à l'infinie définie par l'équation $z = 0$. Soit $g : [x, y, z] \longrightarrow \frac{x}{z}$. Alors g est une paramétrisation affine des

coordonnées $[x, y, z]$ en les coordonnées $[x, y, 1]$. En effet, si $P(x, y, z)$ est une fonction rationnelle de $\mathcal{C} \setminus \text{Sing}(\mathcal{C})$, on a si $z \neq 0$ que

$$P(x, y, z) = P\left(\frac{x}{z}, \frac{y}{z}, 1\right)$$

et donc l'intégrale de fdg devient

$$\int_\gamma fdg = \int_\gamma R(x, y)dg$$

où $R(x, y)$ est une fonction rationnelle où y est une fonction de x définie par l'équation $P(x, y, 1) = 0$. Ainsi, il existe une différentielle méromorphe donnée en coordonnée inhomogène par $y^{-1}dx$.

Considérons maintenant le cas particulier où $\mathcal{C}$ est une cubique non-singulière de $\mathbb{P}_2$ définie par

$$y^2z = 4x^3 - g_2xz^2 - g_3z^3$$

où g_2 et g_3 sont les constantes définies en 2.2.3 qui dépendent du réseau Λ. On sait dans ce cas qu'il existe un biholomorphisme $u : \mathbb{C}/\Lambda \longrightarrow \mathcal{C}_\Lambda$. Par ce qu'on a dit ci-dessus, il existe une différentielle méromorphe sur $\mathcal{C}_\Lambda$ donnée par $y^{-1}dx$. Soit $\pi : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda$ la projection canonique. On considère la différentielle holomorphe

$$\eta = u^*(y^-1dx)$$

On a alors :

$$\begin{aligned}
\pi^*\eta &= \pi^*u^*(y^{-1}dx) \\
&= (u \circ \pi)^*(y^{-1}dx) \\
&= u^*(y^{-1}dx) \\
&= (\wp')^{-1}d\wp \\
&= (\wp')^{-1}\wp'dz \\
&= dz
\end{aligned}$$

avec $z : \mathbb{C} \longrightarrow \mathbb{C}$ est l'identité complexe. Ainsi, comme dz est une différentielle holomorphe et que π est localement une bijection holomorphe d'inverse holomorphe, on en déduit que η est une différentielle holomorphe sur $\mathbb{C}/\Lambda$. Comme u est un biholomorphisme, on en déduit que $y^{-1}dx$ est une différentielle holomorphe sur $\mathcal{C}_\Lambda$ et on peut donc intégrer par rapport ces différentielles.

On va montrer une caractérisation de Λ en terme d'intégrale dépendant de la différentielle η.

Propriété 4.1.6. *Soit Λ un réseau de $\mathbb{C}$. On a*

$$\Lambda = \left\{ \int_\gamma \eta \mid \gamma \textit{ est un lacet } \mathcal{C}^1 \textit{ par morceau de } \mathbb{C}/\Lambda \right\}$$

Démonstration : Considérons $\lambda \in \Lambda$ et soit $\tilde{\gamma} : [0,1] \longrightarrow \mathbb{C}$ le chemin défini par $\tilde{\gamma}(t) = \lambda t$. Soit de plus $\gamma = \pi \circ \tilde{\gamma}$. γ est bien un chemin $\mathcal{C}^1$ par morceau de $\mathbb{C}/\Lambda$ et on a

$$\gamma(0) = \Lambda + 0 = \Lambda + \lambda = \gamma(1)$$

et donc γ est un lacet de $\mathbb{C}/\Lambda$. On a donc

$$\int_\gamma \eta = \int_{\tilde{\gamma}} \pi^*\eta = \int_{\tilde{\gamma}} dz = \tilde{\gamma}(1) - \tilde{\gamma}(0) = \lambda$$

Ainsi, si $\lambda \in \Lambda$, on peut l'envoyer sur le lacet γ et on a ainsi la première inclusion.

Pour la suite, on admettra le résultat suivant : soit $\pi : Y \longrightarrow X$ un revêtement de X et soit $\gamma : [a,b] \longrightarrow X$ un chemin sur X issu de x et soit $y \in Y$ tel que $\pi(y) = x$. Alors il existe une unique application $\tilde{\gamma} : I \longrightarrow Y$ telle que $\gamma = \pi \circ \tilde{\gamma}$ et telle que $\tilde{\gamma}(a) = y$.

Soit $\gamma : [a,b] \longrightarrow \mathbb{C}/\Lambda$ un lacet sur le tore complexe. Par le résultat ci-dessus, il existe un unique lacet dans $\mathbb{C}$ noté $\tilde{\gamma}$ tel que $\pi \circ \tilde{\gamma} = \gamma$. $\tilde{\gamma}$ est $\mathcal{C}^1$ par morceau car π est localement une bijection holomorphe. Alors,

$$\pi \circ \tilde{\gamma}(b) = \gamma(b) = \gamma(a) = \pi \circ \tilde{\gamma}(a)$$

On a ainsi que

$$\int_\gamma \eta = \int_{\tilde{\gamma}} \pi^*\eta = \int_{\tilde{\gamma}} dz = \tilde{\gamma}(b) - \tilde{\gamma}(a) \in \Lambda \quad \square$$

Comme $\eta = u^*(y^{-1}dx)$ et que u est un biholomorphisme, on en déduit le corollaire suivant.

Corollaire 4.1.7. *Soit Λ un réseau de $\mathbb{C}$. On a*

$$\Lambda = \left\{ \int_\gamma y^{-1}dx \mid \gamma \text{ est un lacet } \mathcal{C}^1 \text{ par morceau sur } \mathcal{C}_\Lambda \right\}$$

On peut ainsi facilement retrouver le réseau à l'aide d'intégration sur la courbe elliptique. En passant, nous pouvons aussi expliciter l'inverse du biholomorphisme u sans trop d'efforts.

Propriété 4.1.8. *Soit u le biholomorphisme définit au théorème 3.3.3. Alors u^{-1} est donné par*

$$u^{-1}(p) = \Lambda + \int_{[0,1,0]}^{p} y^{-1}dx$$

Démonstration : Soit $p = u(\Lambda + z)$ et soit $\gamma : [a, b] \longrightarrow \mathcal{C}_\Lambda$ un chemin continu allant de $[0, 1, 0]$ à p. Alors $u^{-1} \circ \gamma$ est un chemin de $\mathbb{C}/\Lambda$ allant de $\Lambda + 0$ à $\Lambda + z$ et on a

$$\begin{aligned}\int_\gamma y^{-1}dx &= \int_{u^{-1}\circ\gamma} u^*(y^{-1}dx) \\ &= \int_{u^{-1}\circ\gamma} \eta \\ &= \tilde{\gamma}(b) - \tilde{\gamma}(a)\end{aligned}$$

où $\tilde{\gamma}$ est un chemin de $\mathbb{C}$ vérifiant $\pi \circ \tilde{\gamma} = u^{-1} \circ \gamma$. Mais alors

$$\begin{aligned}\Lambda + \tilde{\gamma}(b) &= u^{-1}(p) = \Lambda + z \\ \Lambda + \tilde{\gamma}(a) &= u^{-1}([0, 1, 0]) = \Lambda + 0\end{aligned}$$

On obtient alors que

$$\Lambda + \int_\gamma y^{-1}dx = \Lambda + \tilde{\gamma}(b) - \tilde{\gamma}(a) = \Lambda + z = u^{-1}(p)$$

ce qui démontre la propriété. □

4.2 Le théorème de Riemann-Roch

Dans cette partie, nous allons introduire le vocabulaire et les propriétés qui vont nous permettre d'énoncer le théorème de Riemann-Roch, qui sera démontré au paragraphe 4.3. Cette étude se base sur la partie 6.3 de [1]. On va commencer par introduire la notion de diviseur sur une courbe projective complexe.

Définition 4.2.1. *Soit $\mathcal{C}$ une courbe projective complexe. Un diviseur D est une somme formelle*

$$D = \sum_{p\in\mathcal{C}} n_p p$$

tel que $n_p \in \mathbb{Z}$ et $n_p = 0$ pour tout les p sauf un nombre fini d'entre-eux. On définit le degré d'un diviseur D comme étant

$$\deg(D) = \sum_{p\in\mathcal{C}} n_p$$

Soit D un diviseur et numérotons $p_1, \ldots, p_k \in \mathcal{C}$ les éléments tels que $n_{p_i} \neq 0$. Alors on écrira aussi

$$D = \sum_{i=1}^{k} m_i p_i$$

où $m_i = n_{p_i}$. Par convention, on écrira p_i plutôt que $1p_i$ si $m_i = 1$. Si $n_p = 0$ pour tout $p \in \mathcal{C}$, alors on écrira que $D = 0$. On peut, de plus, soustraire des diviseurs entre-eux. Ainsi, en notant $\mathrm{Div}(\mathcal{C})$

l'ensemble des diviseurs sur $\mathcal{C}$, on vient de munir $\mathrm{Div}(\mathcal{C})$ d'une structure de groupe abélien. De plus, il est clair que le degré d'un diviseur définit un morphisme $\deg : \mathrm{Div}(\mathcal{C}) \longrightarrow \mathbb{Z}$.

Si $n_p \geq 0$ pour tout $p \in \mathcal{C}$, on dira que D est positif (ou effectif) et on le notera $D \geq 0$. On écrira $D \geq D'$ si $D - D' \geq 0$. Si $D \geq D'$, alors on a que $\deg(D) \geq \deg(D')$.

Soit f une fonction méromorphe non identiquement nulle sur $\mathcal{C}$ et soit $p \in \mathcal{C}$. Alors il existe $\phi_a : U_a \longrightarrow V_a$ tel que $p \in U_a$. Dans ce cas, $f \circ \phi_a^{-1}$ est une fonction méromorphe sur $V_a \subset \mathbb{C}$. Si $m > 0$, on dit que f a un pôle d'ordre m en p si $f \circ \phi_a^{-1}$ a un pôle d'ordre m au voisinage de $\phi_a(p)$. De même, f possède un zéro d'ordre m en p si $f \circ \phi_a^{-1}$ a un zéro d'ordre m en $\phi_a(p)$. Notons que cette définition ne dépend pas de la carte choisie.

De manière similaire, si $\eta = f dg$ est une différentielle holomorphe non identiquement nulle, on dira que η possède un pôle ou un zéro d'ordre m en p si la fonction

$$(f \circ \phi_a^{-1})(g \circ \phi_a^{-1})'$$

a un zéro ou un pôle d'ordre m en $\phi_a(p)$. Encore une fois, cette définition ne dépend pas de la carte choisie.

Notons que si X est une surface de Riemann compact, alors si f est une fonction méromorphe sur X, elle ne possède qu'un nombre fini de pôles ou de zéros. On peut ainsi définir le diviseur d'une fonction méromorphe sur une courbe $\mathcal{C}$.

Définition 4.2.2. *Soit $\mathcal{C}$ une courbe projective complexe et f une fonction méromorphe non-identiquement nulle sur $\mathcal{C}$. On appelle diviseur de f le diviseur*

$$(f) = \sum_{p \in \mathcal{C}} n_p p$$

où $n_p = m$ si p est un zéro d'ordre m de f et $n_p = -m$ si p est un pôle d'ordre m de f.

À partir de cette définition, et en notant que si f a un pôle (resp. un zéro) d'ordre m en p alors $\frac{1}{f}$ a un zéro (resp. un pôle) d'ordre m en p, on a que

$$(fg) = (f) + (g)$$

$$\left(\frac{f}{g}\right) = (f) - (g)$$

Quelques remarques en vrac :

1. On dira d'un diviseur D qu'il est principal s'il existe une fonction méromorphe f telle que $(f) = D$.
2. On dira de deux diviseurs D et D' qu'ils sont linéairement équivalents si $D - D'$ est un diviseur principal. On notera cette relation $D \sim D'$.
3. On obtient une définition similaire à la définition 4.2.2 en remplaçant la fonction méromorphe f par une forme différentielle holomorphe η. On appellera diviseur canonique tout diviseur D qui est le diviseur d'une forme différentielle méromorphe.

4. Si η et ζ sont deux formes différentielles méromorphes, alors on a vu en partie 4.1 qu'il existait une fonction méromorphe f telle que $\eta = \zeta f$. Ainsi, on a

$$(\eta) = (\zeta) + (f) \sim (\zeta)$$

et donc tout les diviseurs de formes différentielles méromorphes sont linéairement équivalents. On appelle *diviseur canonique* le diviseur d'une forme différentielle méromorphe et on le notera en général κ.

On introduit ici une propriété qui donne une condition nécessaire pour qu'un diviseur soit un diviseur principal. On montrera cette propriété dans la section 4.2.3 du mémoire.

Propriété 4.2.3. *Soit D un diviseur principal sur $\mathcal{C}$. Alors $\deg(D) = 0$. Ainsi, une fonction méromorphe sur $\mathcal{C}$ non-nulle a exactement le même nombre de zéros et de pôles en comptant la multiplicité.*

Une conséquence directe de cette proposition est que tout les diviseurs linéairement équivalents ont le même degré. Ainsi, on obtient que tout les diviseurs canoniques ont le même degré.

Dans la suite, nous aurons besoin de la notion de *genre* d'une courbe. Nous n'irons pas très en profondeur dans cette notion [7]. L'idée intuitive à avoir par rapport à celle-ci est que le genre compte le nombre de "trous" d'une surface. Ainsi, un tore complexe est une surface de genre 1. Nous admettrons la formule suivante, qui donne le genre d'une courbe complexe projective.

Théorème 4.2.4. *Soit $\mathcal{C}$ une courbe complexe projective de degré d. Alors son genre g est donné par la formule suivante*

$$g = \frac{1}{2}(d-1)(d-2)$$

Il nous reste que quelques définitions à donner avant de pouvoir énoncer le théorème de Riemann-Roch.

Définition 4.2.5. *Soit $D = \sum_{p \in \mathcal{C}} n_p p$ un diviseur sur $\mathcal{C}$. On note $\mathcal{L}(D)$ l'ensemble constitué de la fonction nulle et de toute les fonctions méromorphes f sur $\mathcal{C}$ qui vérifient*

$$(f) + D \geq 0$$

On remarque dès lors que $\mathcal{L}(D)$ est un $\mathbb{C}$-espace vectoriel et on pose

$$l(D) = \dim \mathcal{L}(D) \in \mathbb{N} \cup \{\infty\}$$

Si ω est une forme différentielle méromorphe et si f est une fonction méromorphe, alors $(f)+(\omega) \geq 0$ si et seulement si $f\omega$ est une différentielle holomorphe.

C'est direct en appliquant la définition d'un diviseur positif. Ainsi, on peut sans ambiguïté défini l'espace vectoriel des formes différentielles holomorphes de diviseur canonique κ, dont on notera la dimension $l(\kappa)$.

Nous allons maintenant démontrer quelques propriétés qui découlent directement de la propriété 4.2.3.

Propriété 4.2.6. *Soit D un diviseur de $\mathcal{C}$ tel que $\deg(D) < 0$. Alors $l(D) = 0$.*

7. On renvoie à [1], page 85, pour plus d'information sur le genre d'une courbe

Démonstration : Supposons par l'absurde que $l(D) > 0$. Alors il existe $f \in \mathcal{L}(D)$ qui ne soit pas identiquement nulle. Ainsi, on a

$$D + (f) \geq 0$$

Or, on sait que $\deg(f) = 0$ par la proposition 4.2.3. En utilisant le fait que le degré est un morphisme de groupe, on a

$$\deg(D) = \deg(D) + \deg(f) = \deg(D + (f)) \geq 0$$

ce qui est en contradiction avec le fait que $\deg(D) < 0$. □

On va maintenant démontrer un lemme qui nous sera très utile dans la suite.

Lemme 4.2.7. *Soient D et D' deux diviseurs tels que $D \sim D'$. On a alors $l(D) = l(D')$.*

Démonstration : Plus précisément, on va montrer que $\mathcal{L}(D)$ est isomorphe à $\mathcal{L}(D')$. Comme $D \sim D'$, il existe une fonction méromorphe g telle que $D = D' + (g)$.

On considère l'application $\phi : \mathcal{L}(D) \longrightarrow \mathcal{L}(D')$ définie par

$$\phi(f) = fg$$

ϕ est bien définie et est une application linéaire entre espaces vectoriels complexes. C'est de plus une bijection d'inverse $\phi^{-1}(f) = \frac{f}{g}$. Ainsi, $\mathcal{L}(D)$ et $\mathcal{L}(D')$ sont isomorphes et on obtient le résultat attendu de l'énoncé. □

On peut maintenant énoncer le théorème de Riemann-Roch dans le cadre des courbes projectives non-singulières de $\mathbb{P}_2$.

Théorème 4.2.8 (Théorème de Riemann-Roch)**.** *Soit $\mathcal{C}$ une courbe projective non-singulière de $\mathbb{P}_2$. Soit g son genre et soit κ un diviseur canonique de $\mathcal{C}$. On a alors*

$$l(D) - l(\kappa - D) = \deg(D) + 1 - g$$

4.3 Démonstration du théorème de Riemann-Roch

Cette section sera entièrement dédiée à la démonstration du théorème de Riemann-Roch. Celle-ci s'effectuera en plusieurs étapes. On va d'abord énoncer deux lemmes puis montrer le théorème dans le cas où ces deux lemmes sont vrais, puis nous démontrerons ces deux lemmes. Cette démonstration se base sur ce qui est fait dans la partie 6.3 de [1].

Avant cela, nous auront besoin d'une définition.

Définition 4.3.1.

1. *On appelle droite de $\mathbb{P}_2$ tout ensemble L définit comme le lieu d'annulation d'un polynôme homogène $R(x, y, z)$ de degré 1.*
2. *Soit $\mathcal{C}$ une courbe projective complexe donnée par le polynôme P et $[a, b, c]$ un point de $\mathcal{C}$. On écrit $P = P_1 + \cdots + P_m$ comme somme de polynôme homogène de degrés i (on peut avoir $P_i = 0$). On définit la multiplicité du point $[a, b, c]$ comme étant le plus petit i tel que $P_i \neq 0$.*

3. *Soit $p \in \mathbb{P}_2$ et L une droite de $\mathbb{P}_2$. On note $I_p(\mathcal{C}, L)$ la quantité définit comme la multiplicité de l'intersection en p des courbes $\mathcal{C}$ et L.*

Notons que la définition de multiplicité ne dépend que du polynôme P définissant la courbe. On renvoie à [2], page 113, afin d'en avoir une démonstration.

Nous allons étudier un exemple qui nous sera utile dans la preuve du corollaire 4.3.5. Nous aurons besoin pour cela de plus d'informations sur la quantité $I_p(\mathcal{C}, L)$. Pour cela, on admettra le théorème de Bézout [8].

Théorème 4.3.2 (Théorème de Bézout)**.** *Soit $\mathcal{C}$ et $\mathcal{D}$ deux courbes projectives de degré n et m sur $\mathbb{P}_2$ qui n'ont pas de composantes communes. Alors $\mathcal{C}$ et $\mathcal{D}$ ont exactement mn points d'intersection, en comptant la multiplicité i.e*

$$\sum_{p \in \mathcal{C} \cup \mathcal{D}} I_p(\mathcal{C}, \mathcal{D}) = mn$$

Exemple : Soit L une droite donnée par le polynôme $R(x, y, z)$ et $\mathcal{C}$ une courbe projective complexe de degré d donnée par le polynôme $P(x, y, z)$. Considérons le diviseur

$$H = \sum_{p \in \mathcal{C}} I_p(\mathcal{C}, L)p$$

D'après le théorème de Bézout, $\deg(H) = d$. Pour $m \in \mathbb{N}$, on a alors

$$\deg(\kappa - mH) = \deg(\kappa) - md$$

Pour m assez grand, on va avoir $\deg(\kappa - mH) < 0$, donc par la propriété 4.2.6 on aura

$$l(\kappa - mH) = 0$$

On considère dans la suite un tel entier m. Soit $Q(x, y, z)$ un polynôme homogène de degré m. Alors

$$f = \frac{Q(x, y, z)}{R(x, y, z)^m}$$

définit une fonction méromorphe f sur $\mathcal{C}$ qui vérifie

$$(f) + mH \geq 0$$

et donc $f \in \mathcal{L}(mH)$. De plus, on sait que deux tels polynômes définissent la même fonction sur $\mathcal{C}$ si et seulement si leurs différence est divisible par $P(x, y, z)$. On note $C_k[x, y, z]$ l'espace vectoriel des polynômes homogènes de degré d. On a alors, en utilisant notamment le théorème 4.2.4, que

8. On renverra à [1], page 52, pour plus de détails quant à ce théorème.

$$\begin{aligned} l(mH) - l(\kappa - mH) = l(mH) &\geq \dim(C_m[x,y,z]/P(x,y,z)C_{m-d}[x,y,z]) \\ &= \dim C_m[x,y,z] - \dim C_{m-d}[x,y,z] \\ &= \frac{1}{2}(m+1)(m+2) - \frac{1}{2}(m-d+1)(m-d+2) \\ &= md + \frac{1}{2}d(3-d) \\ &= md + 1 - g \end{aligned}$$

On obtient ainsi la première inégalité de Riemann-Roch dans un cas particulier. Notons que, grâce au théorème de Riemann-Roch, l'inégalité devient une égalité et comme $C_m[x,y,z]/P(x,y,z)C_{m-d}[x,y,z]$ est un sous-espace vectoriel de dimension $md+1-g$, on en déduit que $\mathcal{L}(mH)$ est exactement constitué de fonctions rationnelles.

On va maintenant énoncer les deux lemmes qui nous permettront de démontrer le théorème de Riemann-Roch.

Lemme 4.3.3. *Soit D un diviseur de $\mathcal{C}$, L une droite de $\mathbb{P}_2$ et $m_0 \in \mathbb{N}$. On définit le diviseur*

$$H = \sum_{p \in \mathcal{C}} I_p(\mathcal{C}, L)p$$

Alors il existe $m \geq m_0$ et des points $p_1, \ldots, p_k \in \mathcal{C}$ non nécessairement distincts tels que

$$D + p_1 + \cdots + p_k \sim mH$$

Lemme 4.3.4. *Soit D un diviseur de $\mathcal{C}$, κ un diviseur canonique et $p \in \mathcal{C}$. On a alors*

$$0 \leq l(D+p) - l(\kappa - D - p) - l(D) + l(\kappa - D) \leq 1$$

À l'aide de ces deux lemmes, on peut démontrer une des inégalités du théorème de Riemann-Roch.

Corollaire 4.3.5. *Avec les mêmes notations que dans le théorème 4.2.8, on a*

$$l(D) - l(\kappa - D) \geq \deg(D) + 1 - g$$

Démonstration du corollaire 4.3.5 : On a vu dans l'exemple suivant le théorème 4.3.2 qu'il existe un entier positif m_0 tel que pour tout $m \geq m_0$, on a

$$l(mH) - l(\kappa - mH) \geq \deg(mH) + 1 - g$$

Par le lemme 4.3.3, on peut choisir $m \geq m_0$ et des points $p_1, \ldots, p_k \in \mathcal{C}$ tels que

$$D + p_1 + \cdots + p_k \sim mH$$

Ainsi, par la propriété 4.2.3,

$$\deg(mH) = \deg(D + p_1 + \cdots + p_k) = \deg(D) + k$$

et donc, par le lemme 4.2.7, on a

$$l(mH) - l(\kappa - mH) = l(D + p_1 + \cdots + p_k) - l(\kappa - D - p_1 - \cdots - p_k)$$

En utilisant le lemme 4.3.4 et par une rapide récurrence, on a

$$0 \leq l(D + p_1 + \cdots + p_k) - l(\kappa - D - p_1 - \cdots - p_k) - l(D) + l(\kappa - D) \leq k$$

Ainsi, en combinant les inégalités, on obtient que

$$\begin{aligned} l(D) - l(\kappa - D) &\geq l(D + p_1 + \cdots + p_k) - l(\kappa - D - p_1 - \cdots - p_k) - k \\ &= l(mH) - l(\kappa - mH) - k \\ &\geq \deg(mH) + 1 - g - k \\ &= \deg(D) + 1 - h \end{aligned}$$

Ce qui termine la preuve. □

On va maintenant énoncer une propriété qui lie le genre g d'une courbe avec le degré commun aux diviseurs canoniques sur la courbe. Cette propriété sera démontrée plus tard dans cette section.

Propriété 4.3.6. *Soit κ un diviseur canonique sur $\mathcal{C}$. On a alors*

$$\deg(\kappa) = 2g - 2$$

À noter que nous aurions très bien pu définir le genre à l'aide de cette formule, étant donné que tout les diviseurs canoniques ont le même degré par la propriété 4.2.3.

On va maintenant pouvoir démontrer le théorème de Riemann-Roch sachant les lemmes 4.3.3, 4.3.4, le corollaire 4.3.5 et la propriété 4.3.6.

Démonstration du théorème de Riemann-Roch : Le corollaire 4.3.5 nous donne la première inégalité dans le théorème de Riemann-Roch. Il suffit donc de démontrer que

$$l(D) - l(\kappa - D) \leq \deg(D) + 1 - g$$

Or, le corollaire 4.3.5 nous donne que

$$l(\kappa - D) - l(D) \geq \deg(\kappa - D) - g + 1$$

Par la propriété 4.3.6, on a que

$$\begin{aligned} l(\kappa - D) - l(d) &\geq \deg(\kappa - D) - g + 1 \\ &= \deg(\kappa) - \deg(D) - g + 1 \\ &= 2g - 2 - \deg(D) - g + 1 \\ &= -\deg(D) + g - 1 \end{aligned}$$

D'où la seconde inégalité de Riemann-Roch. □

Il nous faut maintenant démontrer les propriétés 4.2.3, 4.3.6 et les lemmes 4.3.3 et 4.3.4. On va commencer par la preuve du lemme 4.3.3.

Démonstration du lemme 4.3.3 : Soit

$$D = \sum_{p \in \mathcal{C}} n p_p$$

un diviseur de D. Il suffit de montrer la propriété dans le cas ou $D \geq 0$ et où $\deg(D) \geq m_0$. En effet, supposant le lemme connu dans ce cas, on peut écrire

$$D = D^+ + D^-$$

où $D^+ \geq 0$ et $D^- \leq 0$. En appliquant le lemme deux fois à D^+ et à D^-, on obtient bien le lemme 4.3.3 dans le cas général. Soit $p \in \mathcal{C}$ tel que $n_p > 0$. Alors il existe une droite L qui coupe $\mathcal{C}$ en p. On note les points d'intersections de L $\mathcal{C}$ (qui sont en nombre fini, et en comptant la multiplicité) $q_i^{(p)}$. On considérera que $q_i^{(p)} = p$.

On sait par le théorème de Bézout que toute droite L coupe $\mathcal{C}$ en d points (comptés avec multiplicité) où d est le degré du polynôme homogène associé à $\mathcal{C}$. Ainsi, si $q_1, \ldots, q_d$ sont les points d'intersection de $\mathcal{C}$ avec n'importe quelle droite, on a

$$q_1 + \cdots + q_d \sim H$$

où H est définit dans l'énoncé du lemme. Soit $m = \deg(D) \geq m_0$. On a alors

$$\begin{aligned} mH &\sim \sum_{i=1}^{d} m q_i \\ &\sim \sum_{i=1}^{d} m q_i^{(p)} \\ &\sim \sum_{n_p > 0} n_p \sum_{i=1}^{d} q_i^{(p)} \\ &= D + p_1 + \cdots + p_k \end{aligned}$$

et ce pour des p_i adaptés et où $k = m(d-1)$. □

On va maintenant démontrer la propriété 4.3.6 sachant la propriété 4.2.3 afin de n'avoir qu'à montrer la propriété 4.2.3.

Démonstration de la propriété 4.3.6 sachant la propriété 4.2.3 : D'après la propriété 4.2.3, il suffit de montrer qu'il existe une forme différentielle ω telle que

$$\deg(\omega) = 2g - 2$$

Soit P un polynôme homogène de degré d qui définit la courbe $\mathcal{C}$. On suppose que l'on a choisi un système de coordonné tel que $[0, 1, 0] \notin \mathcal{C}$. Ainsi, le coefficient dans P de y^d est non-nul et donc $\frac{\partial P}{\partial y} \neq 0$. Par le théorème de Bézout, comme $\frac{\partial P}{\partial y} \neq 0$ et que P est irréductible, les courbes $\mathcal{C}$ et $\frac{\partial P}{\partial y}$ ont un nombre fini de points d'intersections et dont $\frac{\partial P}{\partial y}$ ne s'annule qu'en un nombre fini de points.

Comme $[0,1,0] \notin \mathcal{C}$, x et z ne peuvent être nuls en même temps. Ainsi, en effectuant la transformation projective

$$x \mapsto x, \quad y \mapsto y, \quad z \mapsto \alpha x + z$$

on peut supposer sans perte de généralité que si $\frac{\partial P}{\partial y}(a,b,c) = 0$, alors $c \neq 0$.

Soit ω la différentielle méromorphe $d\left(\frac{x}{z}\right)$. Au voisinage d'un point $[a,b,c]$ où $c \neq 0$ et où $\frac{\partial P}{\partial y}(a,b,c) \neq 0$, on peut choisir (c.f preuve du théorème 3.2.10) $\frac{x}{z}$ comme carte holomorphe locale. Ainsi, ω n'a pas de zéros ou de pôles au voisinage de $[a,b,c]$.

Supposons que $\frac{\partial P}{\partial y}(a,b,c) \neq 0$ et que $c = 0$. Alors $a \neq 0$ et on a alors $v = \frac{z}{x}$ qui est une carte locale. Or,

$$\omega = d\left(\frac{1}{v}\right) = \frac{-dv}{v^2}$$

et ainsi ω a un pôle de multiplicité 2. De plus, comme $\frac{\partial P}{\partial y}(a,b,0) \neq 0$ pour $[a,b,0] \in \mathcal{C}$ donne le fait $z = 0$ n'est jamais tangent à $\mathcal{C}$. Ainsi, par le corollaire 3.2.12, il y a exactement d points qui vérifient $\frac{\partial P}{\partial y}(a,b,0) \neq 0$, et donc ce pôle contribue à $-2d$ au degré de ω.

Soit maintenant $[a,b,c] \in \mathcal{C}$ tel que

$$\frac{\partial P}{\partial y}[a,b,c] = 0$$

D'après l'étude faire au paragraphe 3.2, ces points sont exactement les points de ramification de l'application

$$\phi[x,y,z] = [x,z]$$

Par le choix de notre système de coordonnée, on a $c \neq 0$ et donc $\frac{\partial P}{\partial x}[a,b,c] \neq 0$. Par le lemme 3.2.9, on a ainsi $\frac{\partial P}{\partial z}[a,b,c] \neq 0$. Ainsi, l'application

$$u = \frac{y}{z}$$

est une carte holomorphe au voisinage de $[a,b,c]$. Par le théorème des fonctions implicites, il existe une fonction $f(u)$ de $\frac{x}{z}$ telle que

$$P(f(u),u,1) = 0$$

Soit u_0 tel que $f^{(k)}(u_0) = 0$ pour tout $1 \leq k < m$. On dérive l'identité précédente m fois. On obtient alors

$$f^{(m)}(u_0) = -\frac{\frac{\partial^m P}{\partial y^m}(f(u_0),u_0,1)}{\frac{\partial P}{\partial x} f(u_0),u_0,1)}$$

Ainsi, si l'on considère m le plus petit entier tel que $f^{(m)}(u_0) \neq 0$, alors on a que

$$\frac{\partial^m P}{\partial y^m}(f(u_0), u_0, 1) \neq 0$$

Or, on sait que

$$\omega = d(f(u)) = f'(u)du$$

et donc que la multiplicité du zéro de ω est égale à l'indice de ramification de ϕ moins 1. Par les lemmes 3.2.14 et 3.2.15, on peut supposer que les coordonnées ont été prises de sorte à ce qu'il y ait exactement $d(d-1)$ points de ramification et que ω a des zéros de multiplicité 1 en chacun de ces points. Ainsi, ces points contribuent $d(d-1)$ fois au degré de ω. Ainsi, on a

$$\deg(\omega) = d(d-1) - 2d = d(d-3)$$

et on en déduit directement la formule attendue en utilisant, par le théorème 4.2.4, que $g = \frac{(d-1)(d-2)}{2}$. □

Il nous faut donc maintenant démontrer la propriété 4.2.3 et le lemme 4.3.4. Nous reviendrons à la propriété 4.2.3 plus tard. Pour démontrer le lemme 4.3.4, nous allons d'abord énoncer un lemme et montrer le lemme 4.3.4 sachant ce lemme.

Lemme 4.3.7. *Soit ω une différentielle holomorphe sur $\mathcal{C}$ possédant un unique pôle. Alors ce pôle est de multiplicité au moins deux.*

Démonstration du lemme 4.3.4 sachant le lemme 4.3.7 : Soient $\mathcal{C}$ une courbe non-singulière, D un diviseur quelconque de $\mathcal{C}$, $\kappa = (\omega)$ un diviseur canonique $p \in \mathcal{C}$. On veut montrer que

$$0 \leq l(D+p) - l(\kappa - p - D) - l(D) + l(\kappa - D) \leq 1$$

Soit $D = \sum_{q \in \mathcal{C}} n_q q$. On a l'égalité

$$\mathcal{L}(D+p) = \mathcal{L}(D)$$

si et seulement si il n'existe pas de fonction méromorphe f sur $\mathcal{C}$ telle que

$$(f) + D + p \geq 0$$

où on a l'égalité si f possède un pôle d'ordre $n_p + 1$ en p ou un zéro d'ordre $-n_p - 1$. Sinon, $\mathcal{L}(D+p)$ est un sous-espace vectoriel de $\mathcal{L}(D)$ de codimension 1. Ainsi, on a

$$0 \leq l(D+p) - l(D) \leq 1$$

et, de manière équivalente, on a

$$0 \leq l(\kappa - D) - l(\kappa - D - p) \leq 1$$

Il suffit donc de montrer que l'on ne peut pas avoir simultanément les égalités

$$l(D+p) - l(D) = 1$$
$$l(\kappa - D) - l(\kappa - D - p) = 1$$

Supposons par l'absurde que ces deux égalités soient en même temps vérifiées. Alors il existe deux fonctions méromorphes f et g telles que

$$(f) + D + p \geq 0$$
$$(g) + \kappa - D \geq 0$$
$$g(p) \neq 0$$

Considérons la différentielle méromorphe $fg\omega$. Cette dernière vérifie

$$(fg\omega) = (f) + (g) + \kappa \geq -p$$

et ainsi cette différentielle possède un unique pôle d'ordre 1 en p, ce qui contredit le lemme 4.3.7. □

Afin de démontrer le lemme 4.2.7, nous aurons besoin de la notion de *triangularisation* d'une courbe projective complexe.

Définition 4.3.8. *Soit $\mathcal{C}$ une courbe projective complexe. Une triangularisation de $\mathcal{C}$ est la donnée de*

1. *Un ensemble non-vide V d'éléments appelés sommets.*
2. *Un ensemble non-vide E d'applications continues $e : [0,1] \longrightarrow \mathcal{C}$ appelées arêtes.*
3. *Un ensemble non-vide F d'applications continues $f : \Delta \longrightarrow \mathcal{C}$ appelées faces.*

Ces trois ensembles doivent de plus vérifier les propriétés suivantes :

1. $V = \{e(0) \mid e \in E\} \cup \{e(1) \mid e \in E\}$.
2. *Si $e \in E$, alors la restriction de e à l'intervalle $]0,1[$ est un homéomorphisme sur son image dans $\mathcal{C}$, et cette image ne contient aucun point de V et n'est pas dans l'image d'aucun autre $\tilde{e} \in E$.*
3. *Si $f \in F$, alors la restriction de f à $\mathring{\Delta}$ est un homéomorphisme de $\mathring{\Delta}$ sur une composante connexe K_f de $\mathcal{C} \setminus \Gamma$ où*

$$\Gamma = \bigcup_{e \in E} e([0,1])$$

est l'union des arêtes. De plus, si $r : [0,1] \longrightarrow [0,1]$ et si $\sigma_i : [0,1] \longrightarrow \Delta$ pour $1 \leq i \leq 3$ sont définis par

$$r(t) = 1 - t, \quad \sigma_1(t) = (t, 0), \quad \sigma_2(t) = (1-t, t), \quad \sigma_3(t) = (0, 1-t)$$

alors soit $f \circ \sigma_i$ soit $f \circ \sigma_i \circ r$ est une arête e_f^i pour $1 \leq i \leq 3$.

4. *L'application $f \longrightarrow K_f$ est une bijection.*
5. *Pour tout $e \in E$, il existe une unique face $f_e^+ \in F$ telle que $e = f_e^+ \circ \sigma_i$ pour un certain i. De même, il existe une unique face $f_e^- \in F$ telle que $e = f_e^- \circ \sigma_i$ pour un certain i.*

Remarque : Comme $\mathcal{C}$ est compacte, on peut se convaincre facilement que l'on peut supposer sans perte de généralité que V, E et F sont finis.

Nous allons maintenant énoncer et admettre un lemme sur les triangularisations de $\mathcal{C}$, qui nous permettra enfin (!) de prouver le lemme 4.3.7 et la propriété 4.2.3. Une preuve pourra être trouvée dans [1], page 172.

Lemme 4.3.9. *Soient $\{p_1, \dots, p_r, q_1, \dots, q_s\}$ un ensemble de $r+s$ points de $\mathcal{C}$ avec $r \geq 3$. Alors il existe une triangularisation (V, E, F) de $\mathcal{C}$ telle que $V = \{p_1, \dots, p_r\}$ et telle que les points q_i se trouvent dans une même face i.e qu'il existe $f : \Delta \longrightarrow \mathbb{P}_1$ dans F vérifiant*

$$q_j \in f(\mathring{\Delta})$$

pour $1 \leq j \leq s$. De plus, on peut supposer que ∞ se trouve dans une autre face.

Preuve du lemme 4.3.7 : Soit $\omega = gdh$ une différentielle méromorphe possédant un unique pôle en q. Par l'absurde, supposons que ce pôle est simple. Quitte à changer de coordonnées, on peut supposer que $[0,1,0] \notin \mathcal{C}$. Soit $\phi : [x,y,z] \mapsto [x,z]$. Quitte à de nouveau changer de coordonnées, on peut supposer que 0, ∞ et $\phi(q)$ sont distincts et que ce ne sont pas des points de ramification de ϕ.

Par le lemme 4.3.9, on peut alors trouver une triangularisation (V, E, F) de $\mathbb{P}_1$ tel que tout les points de ramification de ϕ soient dans V, que $\phi(q)$ et 0 soient dans une face f_0 et que ∞ soit dans une face f_∞ (distinctes de f_0). On admettra [9] que les ensembles $(\tilde{V}, \tilde{E}, \tilde{F})$ donnés par

$$\begin{aligned}
\tilde{V} &= \phi^{-1}(V) \\
\tilde{E} &= \{\tilde{e} : [0,1] \longrightarrow \mathcal{C} \mid \tilde{e} \text{ est continue et } \phi \circ \tilde{e} \in E\} \\
\tilde{F} &= \left\{\tilde{f} : \Delta \longrightarrow \mathcal{C} \mid \tilde{f} \text{ est continue et } \phi \circ \tilde{f} \in F\right\}
\end{aligned}$$

forment bien une triangularisation de $\mathcal{C}$. Quitte à rediviser la triangularisation $(\tilde{V}, \tilde{E}, \tilde{F})$, on peut supposer que chaque triangle contient au plus un point de ramification parmi ses sommets. Ainsi, l'application

$$\phi : \tilde{f}(\Delta) \longrightarrow f(\Delta)$$

est un homéomorphisme et sa restriction à $\tilde{f}(\Delta \setminus \{(0,0),(1,0),(0,1)\})$ est la restriction d'une carte holomorphe si $f \neq f_\infty$ (c.f preuve du théorème 3.2.10). Si $f = f_\infty$, il faut composer ϕ par l'application $z \mapsto \frac{1}{z}$.

La frontière de $\tilde{f}(\Delta)$ est l'image des chemins $\tilde{\gamma} = \tilde{f} \circ \sigma_i$ avec σ_i définit en 4.3.8. On voit ainsi que la frontière de $f(\Delta)$ est constitué de l'image des chemins $\gamma = \phi \circ \tilde{\gamma}$. Ainsi, par 4.1.5, on a que

9. On se reportera à [1], page 108, pour la démonstration de ce résultat.

$$\begin{aligned}&\int_{\tilde{\gamma}} \omega \\ &= \int_{\gamma} (\phi^{-1}_{|\tilde{f}(\Delta)})^* \omega \\ &= \int_{\gamma} (g \circ \phi^{-1}_{|\tilde{f}(\Delta)})(h \circ \phi^{-1}_{|\tilde{f}(\Delta)})'(z) dz\end{aligned}$$

Supposons que $q \in \tilde{f}(\mathring{\Delta})$, alors $f = f_0$ et la fonction

$$(g \circ \phi^{-1}_{|\tilde{f}(\Delta)})(h \circ \phi^{-1}_{|\tilde{f}(\Delta)})'$$

possède un unique pôle simple en $\phi(q)$. Comme le résidu d'une fonction ne possédant qu'un pôle simple ne peut être nul, on en déduit du théorème des résidus que

$$\int_{\tilde{\gamma}} \omega \neq 0$$

Réciproquement, si $q \notin \tilde{f}(\mathring{\Delta})$, alors la fonction

$$(g \circ \phi^{-1}_{|\tilde{f}(\Delta)})(h \circ \phi^{-1}_{|\tilde{f}(\Delta)})'$$

ne possède aucun pôle et on en déduit que

$$\int_{\tilde{\gamma}} \omega = 0$$

et ainsi on a

$$\sum_{\tilde{f} \in \tilde{F}} \int_{\tilde{\gamma}} \omega \neq 0$$

De plus, on sait que

$$\int_{\tilde{\gamma}} \omega = \pm \int_{e^1_f} \omega \pm \int_{e^2_f} \omega \pm \int_{e^3_f} \omega$$

où le signe dépend de si $e^i_f = \tilde{f} \circ \sigma_i$ ou si $e^i_f = \tilde{f} \circ \sigma_i \circ r$ (c.f définition 4.3.8). De plus, par définition d'une triangularisation, pour tout $e \in E$, il existe une unique face f^+_e (resp il existe une unique face f^-_e) telle que $e = f^+_e \circ \sigma_i$ (resp telle que $e = f^-_e \circ \sigma_i \circ r$). Ainsi, les intégrales selon les différentes arêtes de

$$\sum_{\tilde{f} \in \tilde{F}} \int_{\tilde{\gamma}} \omega$$

s'annulent entre elles et on en déduit donc que

$$\sum_{\tilde{f} \in \tilde{F}} \int_{\tilde{\gamma}} \omega = 0$$

ce qui est contradictoire. □

Démonstration de la propriété 4.2.3 : Soit D un diviseur principal. On considère une fonction méromorphe f sur $\mathcal{C}$ associée à ce diviseur. Alors f est une fonction holomorphe de $\mathcal{C}$ sur $\mathbb{P}_1$. On note Z (resp P) l'ensemble de ses zéros comptés avec multiplicités (resp l'ensemble de ses pôles comptés avec multiplicité). On a alors d'une part [10]

$$d(f) = \sum_{z \in f^{-1}(0)} \text{mult}_z(f) = |Z|$$

et, d'autre part, on a

$$d(f) = \sum_{z \in f^{-1}(\infty)} \text{mult}_z(f) = |P|$$

Ainsi, on a $|Z| = |P|$ et donc $\deg(D) = 0$. □

4.4 Conséquences du théorème de Riemann-Roch

Nous allons ici montrer, à l'aide du théorème de Riemann-Roch, que nous pouvons adjoindre à une courbe elliptique une unique structure de groupe additif. Cette section a donc uniquement pour but de mettre en avant cette structure de groupe.

Sans plus tarder, énonçons le théorème principal de cette section.

Théorème 4.4.1. *Soit $\mathcal{C}$ une cubique de $\mathbb{P}_2$ et soit $p_0 \in \mathcal{C}$ un point d'inflexion de la courbe $\mathcal{C}$. Il existe une unique structure de groupe abélien sur $\mathcal{C}$ telle que le point p_0 soit l'élément neutre et tels que si $p, q, r \in \mathcal{C}$, alors on a*

$$p + q + r = 0$$

si et seulement si p, q et r sont les trois points d'intersections entre une droite de $\mathbb{P}_2$ et $\mathcal{C}$.

Démonstration : Dans un premier temps, on va montrer que la structure de groupe abélien est unique.

Supposons que l'on ait une autre structure de groupe abélien sur $\mathcal{C}$ qui admette p_0 comme élément neutre et telle que si $p, q, r \in \mathcal{C}$ sont alignées, alors $p + q + r = 0$. Alors si $p \in \mathcal{C}$, comme $p_0 = -p_0$ (car p_0 est le neutre du groupe), on a

$$p_0 + p + (-p) = 0$$

et donc l'inverse de p est nécessairement $-p$. Soient maintenant $p, q \in \mathcal{C}$ tels que $p \neq q$. Alors

$$p + q = -r$$

où $-r$ est le troisième point d'intersection de $\mathcal{C}$ avec la droite où passe p et q (par le théorème de Bézout). Ainsi, toute structure de groupe comme énoncée dans le théorème doit vérifier cela. Enfin,

10. On renvoie à l'annexe B pour les définitions du degré d'une application holomorphe.

si $p = q$, alors $p + q = 0$ et on retrouve le cas précédent. Ainsi, la structure de groupe additif est unique. Il faut maintenant montrer qu'elle existe.

Si $p, q \in \mathcal{C}$, alors la droite passant par p et q et la droite passant par q et p sont les mêmes, on a ainsi la commutativité du groupe.

Soit $p \neq p_0$ un point de $\mathbb{P}_2$. Par le théorème de Bézout, il existe un point $r \in \mathcal{C}$ tel que

$$p + p_0 = -r$$

où r est le troisième point d'intersection entre $\mathcal{C}$ et la droite passant par p et p_0 (comme p_0 est un point d'inflexion, on a $r \neq p_0$). Ainsi, $-r$ est aussi le troisième point d'intersection entre $\mathcal{C}$ et la droite passant par p_0 et r et on a donc

$$r + p_0 + (-r) = 0$$

et on en déduit ainsi que $p = -r$. De plus, $p + p_0 = p$ et $p_0 + p_0 = p_0$. À l'aide de ces propriétés, on en déduit donc que l'addition est bien définie et que tout élément est inversible et que l'inverse de p est $-p$.

Il nous reste à prouver l'associativité du groupe. C'est là que nous avons besoin du théorème de Riemann-Roch. Considérons $p, q, r \in \mathcal{C}$. Soient

$$\begin{aligned} a &= p + q \\ b &= a + r = (p + q) + r \\ c &= q + r \\ d &= p + c = p + (q + r) \end{aligned}$$

Afin de montrer que la loi est associative, il suffit de montrer que $b = d$. Comme p, q et $-a$ sont colinéaires, il existe un polynôme homogène P de degré 1 s'annulant en p, q et $-a$. De même, a, $-a$ et p_0 sont colinéaires donc il existe un polynôme homogène Q de degré 1 s'annulant en ces points. On définit alors la fonction méromorphe

$$\phi = \frac{P}{Q}$$

Cette dernière s'annule en p et q et possède des pôles en a et p_0 (comptés avec multiplicité). De la même façon que précédemment, il existe une fonction méromorphe ϕ s'annulant en a et r et ayant des pôles en b et p_0. Ainsi, le produit $\phi\psi$ est une fonction méromorphe sur $\mathcal{C}$ possédant des zéros en p, q et r et un pôle en p_0 (de multiplicité 2) et en b. De manière similaire, il existe une fonction méromorphe s'annulant en p, q et r, et possédant des pôles en p_0 (de multiplicité 2) et en d.

Supposons par l'absurde que $b \neq d$. Alors le ratio de ces deux fonctions méromorphes possède un zéro d'ordre 1 en b et un pôle simple en d, et aucun autre pôle ou zéro. Par le théorème 4.2.4, le genre d'une cubique est 1. On considère b vu comme un diviseur sur $\mathcal{C}$ et κ un diviseur canonique. Il résulte de la propriété 4.3.6 que

$$\deg(\kappa) = 2g - 2 = 0$$

et donc que $\deg(\kappa - b) < 0$. Ainsi, par la propriété 4.2.6, on a que

$$l(\kappa - b) = 0$$

Le théorème de Riemann-Roch nous donne ainsi que

$$l(b) - l(\kappa - b) = l(b) = \deg(b) + 1 - 1 = 1$$

et donc que les seules fonctions méromorphes sur $\mathcal{C}$ sont les fonctions constantes, ce qui contredit l'existence de la fonction méromorphe construite précédemment. Ainsi, $b = d$ et l'associativité est ainsi prouvée. □

A Rappels sur les fonctions holomorphes

Dans cette section, on rappellera sans démonstration des résultats d'analyse complexe que nous utiliseront tout du long du document. Ces derniers proviennent tous de l'UE *fonctions holomorphes* de M1.

Théorème A.0.1 (de Liouville). *Soit f une fonction holomorphe sur $\mathbb{C}$. Si f est bornée, alors f est constante.*

Théorème A.0.2 (critère de Weierstrass). *Soit $U \subset \mathbb{C}$ un ouvert, et $f_n : U \longrightarrow \mathbb{C}$ une suite de fonctions holomorphes sur U. Supposons qu'il existe une suite réelle $(a_n)_{n\in\mathbb{N}}$ telle que*

$$\sum_{n\geq 0} a_n < +\infty \text{ et que } |f_n(z)| \leq a_n \text{ pour tout } z \in U$$

Alors la série $\sum_{n\geq 0} f_n(z)$ converge uniformément sur U vers une fonction f holomorphe sur U qui vérifie $\forall z \in U,\ f'(z) = \sum_{n\geq 0} f_n'(z)$

Définition A.0.3. *Soit U un ouvert de $\mathbb{C}$. Une fonction $f : U \longrightarrow \mathbb{C} \cup \{\infty\}$ est dite méromorphe sur U si f est holomorphe sur $U \setminus f^{-1}(\{\infty\})$ et si tout les points de $U \setminus f^{-1}(\{\infty\})$ sont des pôles de f.*

Propriété A.0.4 (théorème de l'indice). *Soit U un ouvert étoilé, f une fonction méromorphe sur U possédant un nombre fini de zéros $w_1, \dots, w_k$ et de pôles $w_1, \dots, w_r$ et γ un lacet $\mathcal{C}^1$ par morceau évitant les zéros et les pôles de f.*
La fonction $\frac{f'}{f}$ est méromorphe sur U et a des pôles d'ordre 1 aux points z_j, et on a

$$\frac{1}{2i\pi}\int_\gamma \frac{f'(z)}{f(z)}dz = \sum_{j=1}^{k} \mathrm{Ind}_\gamma(w_j) - \sum_{j=1}^{r} \mathrm{Ind}_\gamma(z_j)$$

En particulier, si tout les indices valent un, on a que

$$\frac{1}{2i\pi}\int_\gamma \frac{f'(z)}{f(z)}dz = Z - P$$

où Z est le nombre de zéros dans le domaine délimité par γ et P le nombre de pôles dans le domaine délimité par γ.

B Surfaces de Riemann

On introduit ici du vocabulaire sur les surfaces de Riemann que nous utiliseront souvent dans ce mémoire. On y retrouvera notamment une preuve du fait qu'un tore complexe est bien une surface de Riemann.

Définition B.0.1. *Soit X un espace topologique séparé et connexe. On dit que X est une surface Riemann si :*

1. *Il existe $(U_i)_{i\in I}$ une famille d'ouverts de X au plus dénombrable qui recouvre X.*
2. *Il existe des fonction $\varphi_i : U_i \longrightarrow \mathbb{C}$ telle que φ_i est un homéomorphisme sur son image.*
3. *Pour tout $i, j \in I$ tels que $i \neq j$ et $U_i \cap U_j \neq \emptyset$, l'application*

$$g_{ij} = \varphi_i \circ \varphi_j^{-1} : \varphi_j(U_i \cap U_j) \longrightarrow \varphi_i(U_i \cap U_j)$$

est holomorphe.

Le couple $(U_i, \varphi_i)_{i\in I}$ est un atlas holomorphe sur X. S'il n'y a pas d'ambiguïté, on dira simplement que c'est un atlas sur X.

Définition B.0.2. *Soit X une surface de Riemann d'atlas (U_i, φ_i), $U \subset X$ un ouvert et $f : U \longrightarrow \mathbb{C}$ une fonction. On dit que f est holomorphe si*

$$\forall i \in I, \quad f \circ \varphi_i^{-1} : \varphi_i(U_i \cap U) \longrightarrow \mathbb{C}$$

est une fonction holomorphe.

Définition B.0.3. *Soient X et Y deux surfaces de Riemann possédant des atlas respectifs (U_i, φ_i) et (V_j, ψ_j). On dit qu'une application continue $f : X \longrightarrow Y$ est holomorphe en $x \in X$ si l'application*

$$\psi_j \circ f \circ \varphi_i^{-1} : \varphi_i(U_i) \longrightarrow \psi_j(V_j)$$

est holomorphe en $\varphi_i(x)$. On dira que f est holomorphe sur X si elle est holomorphe en tout point de x.

On voit que la définition B.0.2 n'est qu'un cas particulier de cette définition, où $Y = \mathbb{C}$ et où l'atlas considéré est uniquement constitué de $\mathbb{C}$ entier muni de l'identité.

Définition B.0.4. *Soient X une surface de Riemann. On dit que deux atlas sur X (U_i, φ_i) et (V_j, ψ_j) sont compatibles si la fonction identité de X munit de l'atlas (U_i, φ_i), à valeur dans X munit de l'atlas (V_i, ψ_i), est holomorphe.*
On vérifie sans problèmes que la relation "être compatible" est une relation d'équivalence sur les atlas holomorphes de X.

On considère que deux atlas holomorphes compatibles définissent la même surface de Riemann. Ainsi, quand on parlera de "surface de Riemann", il faudra comprendre "surface de Riemann à atlas holomorphe compatible près".

Définition B.0.5. *Deux surfaces de Riemann X et Y sont biholomorphes s'il existe une fonction $f : X \longrightarrow Y$ holomorphe bijective d'inverse holomorphe.*

En réalité, on peut se passer de l'hypothèse "d'inverse holomorphe".

Définition B.0.6. *Soit X une surface de Riemann. On dit que la fonction $f : X \longrightarrow \mathbb{P}_1(\mathbb{C})$ est méromorphe si f est holomorphe au sens des surfaces de Riemann et si f n'est pas constante égale à ∞ sur toute composante connexe de X.*

On énonce maintenant plusieurs propriétés quant à la multiplicité et au degré d'une application holomorphe.

Propriété B.0.7 (Multiplicité d'une application holomorphe)**.** *Soit $f : X \longrightarrow Y$ une fonction holomorphe non-constante et soit $x \in X$. Alors il existe $m \geq 1$ tel que, pour toute carte $\psi : V \longrightarrow \mathbb{C}$ avec $f(x) \in V$ et vérifiant $\psi(f(x)) = 0$, il existe une carte $\varphi : U \longrightarrow \mathbb{C}$ avec $x \in U$ tel que si*

$$\tilde{f}(z) = \psi \circ f \circ \varphi^{-1} : \varphi(U) \longrightarrow \psi(V)$$

alors on a

$$\tilde{f}(z) = z^m$$

L'entier m est appelé la multiplicité de f en x et on le note $mult_x(f)$.

Propriété B.0.8 (Degré d'une application holomorphe)**.** *Soit X et Y deux surfaces de Riemann compactes et $f : X \longrightarrow Y$ une fonction holomorphe non-constante. Pour tout $y \in Y$, on définit le degré de f en y comme étant*

$$d_y(f) = \sum_{p \in f^{-1}(y)} mult_p(f)$$

Alors $d_y(f)$ ne dépend pas du point considéré.

Références

[1] Frances Kirwan, *Complex Algebraic Curves*, Cambridge University press, 1992

[2] Daniel Perrin, *Géométrie Algébrique*, 1995

[3] Svetlana Katok, *Fuchsian Groups*, University of Chicago Press, 1992

[4] Allen Hatcher, *Algebraic topology*, 2001, *https ://pi.math.cornell.edu/ hatcher/AT/AT.pdf*

[5] Hershel M. Farkas, Irwin Kra, *Riemann Surfaces*, Graduate Texts in Mathematics, 1992